Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce.

Simson L. Garfinkel[1], Jeffrey I. Schiller[1], Erik Nordlander[1], David Margrave[2], and Robert C. Miller[1]

[1] MIT, Cambridge, MA 02139, USA,
{simsong,jis,erikn,rcm}@mit.edu
[2] Amazon.com, Seattle, WA
DavidMA@amazon.com

Abstract. We surveyed 470 Amazon.com merchants regarding their experience, knowledge and perceptions of digitally-signed email. Some of these merchants (93) had been receiving digitally-signed VAT invoices from Amazon for more than a year. Respondents attitudes were measured as to the role of signed and/or sealed mail in e-commerce. Among our findings: 25.2% of merchants thought that receipts sent by online merchants should be digitally-signed, 13.2% thought they should be sealed with encryption, and 33.6% thought that they should be both signed and sealed. Statistically-significant differences between merchants who had received the signed mail and those who had not are noted. We conclude that Internet-based merchants should send digitally-signed email as a "best practice," even if they think that their customers will not understand the signatures, on the grounds that today's email systems handle such signatures automatically and the passive exposure to signatures appears to increase acceptance and trust.

1 Introduction

Public key cryptography can be used to *sign* a message so that the recepient can verify that the message has not been modified after was sent. Cryptography can also be used to *seal* the contents of an electronic message so that it cannot be deciphered by anyone who does not have a corresponding key — presumably anything other than the intended recipient.

These two cryptographic primitives—signing and sealing—have been at the root of public key cryptography since its invention in the 1970s. Over the past two decades the Internet community has adopted three standards—Privacy Enhanced Mail, OpenPGP, and S/MIME—all of which are designed to allow Internet users to exchange email with integrity and privacy protections. Support for two of these standards, OpenPGP and S/MIME, has been widely available since 1997. Nevertheless, email messages that are either digitally-signed or sealed are a rarity on the Internet today. [1]

The lack of cryptographic participation is all the more surprising when one considers the real need for this technology in today's electronic marketplace:

– Email can easily be modified in transit, misdelivered to the wrong recipient, or copied without the knowledge of the correspondents.

– In recent years Internet users have been beset by a deluge of so-called "phishing" email messages—messages that purport to be from a respected bank or other financial institution that direct the recipients to bandit websites that exist for the purpose of stealing usernames and passwords. [2]
– Many email messages and computer viruses attempt to trick the recipient into opening the message by using a forged "From:" address.

Ironically, these are the very kinds of attacks that were supposed to be prevented by cryptography.

1.1 Usability Barriers

Usability barriers such as difficult-to-use software and confusing terminology [3] are widely perceived as the primary reason why organizations and individuals have not adopted secure messaging technology.

It is easy to understand why usability barriers have affected the exchange of cryptographically sealed mail: two people cannot exchange such messages unless they have compatible software and possess each others' public keys. And even if keys have been exchanged and have been certified, there is always a risk that the recipient will be unable to unseal the message after it is received—perhaps because the key is lost after the message was sent. For messages that do not obviously require secrecy, many correspondents think that the risk of unauthorized interception is not worth the effort of encryption.

Widespread deployment of digitally-signed mail has been blocked by many barriers. An initial barrier was the deployment of four different and mutually-incompatible standards for signed email: Privacy Enhanced Mail [4, 5, 6], PGP clear-signed signatures [7], OpenPGP MIME [8, 9], and S/MIME [10, 11]. The obvious problem caused by competing standards is that there is no guarantee that a signed message, once sent, will be verifiable by the recipient. A deeper problem is that signatures, and sometimes the original email message itself, appear as indecipherable attachments when they are received by email clients that implement the other MIME-based standard.

The wide-scale deployment of mail clients implementing the S/MIME standard has largely solved the standardization problem. Support for S/MIME is built-in to Microsoft Outlook, Outlook Express, Mozilla and Netscape. What's more, keys for several popular certification authorities (CAs), such as VeriSign, are distributed both with these programs and with many popular operating systems. Thus, while *sending* digitally-signed mail is still relatively cumbersome (requiring that the user obtain a key and procure a digital certificate signed by an established CA), there is a high likelihood that properly-signed mail, once sent, can be readily verified. Nevertheless, few individuals or organizations appear to be sending digitally-signed mail.

1.2 Genesis of the Survey

EU Directive 99/93/EU calls for the use of advanced digital signatures for certain kinds of electronic messages. "Advanced digital signatures" are generally taken to mean digital signatures, signed with a private key, that permits the recipient to determine whether or not the contents of the document were modified after the document was sent.

Amazon Services Europe S.à r.l. started sending signed electronic Value Added Tax (VAT) invoices to each of its Amazon Marketplace, Auctions, and zShops sellers in June 2003. Amazon's signatures were S/MIME digital signatures certified by a VeriSign Class 1 Digital ID.

Amazon does not send digitally-signed messages to its sellers operating in America, Asia, and other geographic regions. Because some sellers were receiving signed messages and some were not, we decided to survey Amazon's sellers to discover their reaction to these messages in particular and digitally-signed messages in general.

Digital signatures assure the integrity of email, but did the recipients of the signed email think that such messages were more trustworthy or more likely to be truthful than messages that were not digitally-signed? Did the sellers even know what a digital-signature was, or know that they were receiving them? How did receiving these signatures change the seller's opinion of Amazon? And to what other purposes did the sellers think digital certification should be applied?

1.3 Prior Work

We have found very few published studies of popular attitudes regarding encryption and other security technologies. As previously noted, Gutmann suggests that digitally-signed messages comprise a tiny percentage of the non-spam messages that traverse the Internet each day. [1] The 10th GVU WWW User Survey [12] found that a majority of respondents described themselves very (52.8%) or somewhat (26.7%) concerned about security. Nevertheless, "the most important issue facing the Internet" most frequently selected by GVU's respondents was privacy (19.1%); "security of e-commerce" ranked 8^{th} garnering just 5% of the votes.

Whitten and Tygar's study of PGP 5.0 [3] confirmed popularly-held beliefs that even software with attractive graphical user interfaces can have stunning usability problems. But Whitten and Tygar only measured the difficulty of *sending* encrypted mail and key management; they didn't measure their subjects' ability to *receive* and understand the significance of digitally-signed mail.

2 Methodology

Our survey consisted of 40 questions on 5 web pages. Respondents were recruited through a set of notices placed by Amazon employees in a variety of Amazon Seller's Forums. Participation was voluntary and all respondents were anonymous. Respondents from Europe and The United States were distinguished through the use of different URLs. A cookie deposited on the respondent's web browser prevented the same respondent from easily filling out the survey multiple times.

A total of 1083 respondents clicked on the link that was posted in the Amazon forums in August 2004. Of these, 470 submitted the first web page, and 417 completed all five pages. We attribute this high follow-through rate to the brevity of the survey: each page took on average 2 minutes to complete.

2.1 Characterizing the Respondents

The average age of our respondents was 41.5. Of the 411 responding, 53.5% identified themselves as female, 42.6% as male, and 3.9% chose "Declined to answer." The sample was highly-educated, with more than half claiming to have an advanced degree (26.1%) or a college degree (34.9%), and another 30.0% claiming some college education. More than three quarters described themselves as "very sophisticated" (18.0%) or "comfortable" (63.7%) at using computers and the Internet. Roughly half of the respondents had obtained their first email account in the 1990s, with one quarter getting their accounts before 1990 and one quarter getting their accounts after 1999.

2.2 Segmenting the Respondents

The survey contained four tests for segmenting the respondents:

- We can divide our sample according to whether they accessed the survey from the URL that was posted to the Amazon forums frequented by European sellers or those accessed by American sellers. We call these groups *Europe* and *US*. As noted, Amazon has been sending sellers in the *Europe* group digitally-signed email since June 2003, while those in the *US* group have never been sent digitally-signed email from Amazon. A few recepients of digitally-signed messages sent messages back to Amazon such as "what is this `smime.p7s` attachment? I can't read it!" Nevertheless, the vast majority of them did not comment before the study either favorably or negatively on the digitally-signed messages. There were 93 respondents in the *Europe* group and 376 in the *US* group.
- An alternative partitioning is between respondents who have some experience or stated knowledge with encryption technology and those that do not. We selected respondents who met any of the following criteria:
  - Respondents who had indicated that their "understanding of encryption and digital signatures" was 1 ("very good") or who indicated that their understanding was a 2 on 5-point scale (with 5 listed as "none")—23 and 53 respondents, respectively;[3]
  - Respondents who indicated that they had received a digitally-signed message (104 respondents);
  - Respondents who indicated that they had received a message that was sealed with encryption (39 respondents);
  - Respondents who said they "always," or "sometimes," send digitally-signed messages (29 respondents);

  A total of 148 respondents met one or more of these criteria. We called this the *Savvy* group—they were savvy because they had some experience with encryption

[3] We asked our segmenting questions before defining terms such as *encryption* and *digital signature*. Although this decision resulted in some criticism from respondents, we wanted to select those in the *Savvy* based on their familiarity with the terminology of public key cryptography (e.g. "digitally-sign," "encrypt"), rather than the underlying concepts, since user interfaces generally present the terminology without explanation.

Table 1. "When were your born?"

Group	Year	N	σ
ALL	41.5	407	12.36
Europe	**36.2**	74	10.81
US	**42.7**	333	12.38
Savvy	**38.0**	135	11.74
Green	**43.2**	272	12.28

or had self-identified themselves as knowing more about encryption than the average person. Those individuals not in the *Savvy* group were put in a second group called *Green*.

Thus, the *Europe/US* division measures the impact on attitudes given the actual experience in receiving digitally-signed mail from Amazon, while the *Savvy/Green* division measures the impact of people's stated knowledge of or experience with both digital signatures and message sealing.

Results of partitioning the respondents into two groups are deemed to be statistically significant if a logistic regression based on a Chi-Square test yielded a confidence level of $p = 0.05$ for the particular response in question. Such responses are printed **in bold** and necessarily appear in pairs. Where the confidence level is considerably better than $p = 0.05$ the corresponding confidence level is indicated in a table footnote. The lack of bold type does not indicate that findings are not statistically significant; it merely indicates that there is no statistically-significant difference between the two groups.

We performed analysis in terms of education for our segments. Overall, both the *Europe* and *Savvy* groups were younger (Table 1) and less educated (Table 2) than their *US* and *Green* counterparts—differences that were statistically significant.

Table 2. "What's your highest level of education:"

	ALL	Europe	US	Savvy	Green
Some high school	2%	4%	1%	**4%** *	**1%** *
Completed high school	7%	**16%** **	**5%** **	8%	7%
Some college	30%	27%	31%	31%	29%
College degree	35%	30%	36%	**27%** *	**39%** *
Advanced degree	26%	23%	27%	29%	25%
Total Respondents	410	74	336	137	273
No Response	(7)	(1)	(6)	(1)	(6)

*$p < .05$; **$p < .01$;

As Table 3 shows, many people who had received digitally-signed mail from Amazon were not aware of the fact. The fact that roughly half of these individuals indicated that they had not received such a message suggests that differences in opinion regarding

digitally-signed mail between *Europe* and *US* may be attributable to passively experiencing the little certificates in the user interface that are displayed when programs such as Outlook Express receive digitally-signed messages—and not to any specific instruction or indoctrination about the technology.

Table 3. "What kinds of email have you received? Please check all that apply:"

	ALL	Europe	US
Email that was digitally-signed	22%	**33%** **	**20%** **
Email that was sealed with encryption so that only I could read it.	9%	**16%** *	**7%** *
Email that was both signed and sealed.	7%	10%	6%
I do not think that I have received messages that were signed or sealed.	37%	30%	39%
I have not received messages that were signed or sealed.	21%	23%	20%
I'm sorry, I don't understand what you mean by "signed," "sealed" and "encrypted".	26%	**17%** *	**28%** *
Total Respondents	455	88	367
No Response	(15)	(5)	(9)

*$p < .05$; **$p < .01$;

2.3 Evaluating the Segments

To evaluate our segments, we compared their responses to two test questions. One question asked users, "Practically speaking, do you think that there is a difference between mail that is digitally-signed and mail that is sealed with encryption?" The correct answer was "yes:" sealing renders the message unintelligible to all but the intended recipients, while signatures provide integrity and some assurance of authorship. As shown in Table 4, both *Europe* and *Savvy* demonstrated a significantly higher understanding of digital signatures than *US* or *Green*. (Although we also received a higher percentage of "no" answers, the increase was not statistically significant at $p = 0.05$.)

We also asked respondents if they thought there was a difference between messages that were sealed with encryption and messages that were both signed and sealed. Once again, the answer to this question is "Yes," with both *Europe* and *Savvy* understanding this distinction more than their counterparts, as shown in Table 5.

3 Results

Respondents were asked a variety of questions as to when they thought that it was appropriate to use digital signatures for signing or encryption for sealing electronic mail. They were also asked questions on a 5-point scale regarding their opinion of organizations that send signed mail.

Table 4. "Practically speaking, do you think that there is a difference between mail that is digitally-signed and mail that is sealed with encryption?" [The correct answer is "yes."]

	ALL	Europe	US	Savvy	Green
Yes	54%	**67%** **	**51%** **	**78%** ***	**42%** ***
No	7%	7%	7%	10%	5%
Don't know	39%	**26%** **	**43%** **	**12%** ***	**52%** ***
Total Respondents	452	86	366	146	306
No Response	(18)	(7)	(10)	(2)	(16)

$^{**}p < .01$; $^{***}p < .001$;

Table 5. "Practically speaking, do you think that there is a difference between mail that is sealed with encryption so that only you can read it, and mail that is both sealed for you and signed by the sender so that you can verify the sender's identity." [The correct answer is "yes."]

	ALL	Europe	US	Savvy	Green
Yes	51%	**62%** *	**48%** *	**71%** ***	**41%** ***
No	8%	9%	8%	11%	7%
Don't know	41%	**28%** **	**44%** **	**18%** ***	**53%** ***
Total Respondents	452	85	367	146	306
No Response	(18)	(8)	(9)	(2)	(16)

$^{*}p < .05$; $^{**}p < .01$; $^{***}p < .001$;

3.1 Ability to Validate Digitally-Signed Mail

The first matter of business was to determine whether or not respondents could in fact validate digitally-signed mail. For the majority, the answer was an unqualified "yes:" The vast majority of our respondents used Microsoft Outlook Express (41.8%), Outlook (30.6%), or Netscape (10.1%) to read their mail—all of which can validate email signed with S/MIME signatures. Adding in other S/MIME compatible mail readers such as Apple Mail and Lotus Notes, we found that 81.1% could validate digitally-signed messages.

Many of our users didn't know that they could handle such mail, however. We asked users if their email client handles encryption, giving them allowable answers of "Yes," "No," "I don't know" and "what's encryption?" and found that only 26.9% responded in the affirmative.

3.2 Appropriate Uses of Signing and Sealing

It has long been argued by encryption advocates that encryption should be easy-to-use and ubiquitous — that virtually all digital messages should be signed, at least with anonymous or self-signed keys, and many should be sealed, as well.

Our respondents feel otherwise. When asked what kind of protection is appropriate for email, respondents answered that different kinds of email require different kinds of

protection. In many cases the results of these answers were significantly different for the group that had been receiving digitally-signed messages versus the group that had not been.

Commercially-Oriented Email (Tables 6, 7 and 8) Typical email exchanged between merchants and consumers includes *advertisements* from the merchant to the consumer, *questions* that the consumer may pose the merchant, and *receipts* that the merchant may send the consumer after the transaction takes place. The consumer may send the merchant additional follow-up questions. Given that these are typical kinds of messages our respondents exchange with their customers, we sought to discover what level of security our respondents thought appropriate.

Roughly 29% of all respondents agreed with the statement that advertisements should never be sent by email. (This question did not distinguish between email that should not be sent because it might be considered "spam" and messages that should not be sent by email because their content is too sensitive, but comments from respondents indicated that many took this question to be a question about unsolicited commercial email.)

Very few respondents (14%) thought advertisements should be digitally-signed—a surprising number, considering that forged advertisements would definitely present many merchants with a significant problem. Instead, a majority of respondents (54%) thought that advertisements require no special protection at all.

Likewise, few respondents thought that questions to online merchants required any sort of special protection. Remember, *all respondents in the survey are online merchants* — so these merchants are basically writing about what kind of messages they wish to receive. Interestingly, our two groups with either actual or acknowledged experience thought that questions to merchants required *less protection* than their counterpart groups.

This result is surprising because Europeans are generally thought to be more concerned in the privacy practices of businesses than are Americans. One possible explanation for these results is that experience with digital signatures led the Europeans to conclude that a signed receipt was sufficient protection; another explanation is that a significant number of Americans misunderstood the question.

On the other hand, a majority of all respondents (58.8%) thought that receipts from online merchants should be digitally signed, while a roughly a third (46.8%) thought that receipts should be sealed with encryption. Of course, this is not the case with the vast majority of receipts being sent today.

Personal Email - At Home and Work (Tables 9 and 10) For years advocates of cryptography have argued that one of the primary purposes of the technology is to protect personal email sent or received at home and at work. The respondents to our survey found no strong desire for technical measures to ensure either integrity or privacy. Even more noteworthy, respondents in the *Europe* and *Savvy* groups saw fewer needs for protection than those in the *US* and *Green* group. One explanation for this result is that increased exposure to security technology increases one's confidence in the computer infrastructure — *even when that technology is not being employed.* Another explanation

Table 6. "Advertisements:"

	ALL	Europe	US	Savvy	Green
Does not need special protection	54%	58%	53%	52%	54%
Should be *digitally-signed*	14%	14%	14%	18%	12%
Should be *sealed* with encryption	1%	1%	1%	2%	0%
Should be *both* signed and sealed	3%	1%	3%	2%	3%
Should never be sent by email	29%	26%	30%	26%	30%
sealed or *both*	3%	3%	4%	4%	3%
digitally-signed or *both*	17%	15%	17%	20%	15%
Total Respondents	429	78	351	142	287
No Response	(4)	(2)	(2)	(0)	(4)

Table 7. "Questions to online merchants:"

	ALL	Europe	US	Savvy	Green
Does not need special protection	61%	69%	59%	67%	58%
Should be *digitally-signed*	20%	15%	21%	18%	20%
Should be *sealed* with encryption	5%	6%	5%	6%	5%
Should be *both* signed and sealed	13%	9%	14%	**8%** *	**15%** *
Should never be sent by email	1%	0%	1%	0%	1%
sealed or *both*	18%	15%	19%	14%	20%
digitally-signed or *both*	33%	24%	34%	**26%** *	**36%** *
Total Respondents	426	78	348	141	285
No Response	(7)	(2)	(5)	(1)	(6)

*$p < .05$;

Table 8. "Receipts from online merchants:"

	ALL	Europe	US	Savvy	Green
Does not need special protection	25%	29%	25%	26%	25%
Should be *digitally-signed*	25%	**39%** **	**22%** **	**33%** *	**21%** *
Should be *sealed* with encryption	13%	**6%** *	**15%** *	12%	14%
Should be *both* signed and sealed	34%	**23%** *	**36%** *	**27%** *	**37%** *
Should never be sent by email	3%	3%	3%	2%	3%
sealed or *both*	47%	**30%** ***	**51%** ***	**39%** *	**51%** *
digitally-signed or *both*	59%	62%	58%	60%	58%
Total Respondents	425	77	348	141	284
No Response	(8)	(3)	(5)	(1)	(7)

*$p < .05$; **$p < .01$; ***$p < .001$;

is that generally more stringent privacy legislation in Europe has removed eavesdropping as a concern from many people's minds.

Financial Communications (Table 11) Not surprisingly, a majority (62.7%) of our respondents thought that financial statements should be both signed and sealed. There was

Table 9. "Personal email sent or received at work:"

	ALL	Europe	US	Savvy	Green
Does not need special protection	35%	**47%** *	**33%** *	40%	33%
Should be *digitally-signed*	17%	18%	17%	21%	15%
Should be *sealed* with encryption	15%	17%	14%	**9%** **	**18%** **
Should be *both* signed and sealed	23%	**14%** *	**25%** *	18%	26%
Should never be sent by email	10%	**4%** *	**11%** *	13%	8%
sealed or *both*	38%	31%	39%	**26%** ***	**44%** ***
digitally-signed or *both*	40%	32%	42%	38%	41%
Total Respondents	425	77	348	141	284
No Response	(8)	(3)	(5)	(1)	(7)

*$p < .05$; **$p < .01$; ***$p < .001$;

Table 10. "Personal email sent or received at home:"

	ALL	Europe	US	Savvy	Green
Does not need special protection	51%	58%	49%	53%	49%
Should be *digitally-signed*	18%	16%	18%	22%	16%
Should be *sealed* with encryption	9%	9%	9%	9%	9%
Should be *both* signed and sealed	23%	17%	24%	**17%** *	**25%** *
Should never be sent by email	0%	0%	0%	0%	0%
sealed or *both*	31%	26%	33%	**25%** *	**34%** *
digitally-signed or *both*	40%	32%	42%	38%	41%
Total Respondents	426	77	349	139	287
No Response	(7)	(3)	(4)	(3)	(4)

*$p < .05$;

no significant difference in response rates to this question between any of our groups. Similar response rates were seen for official mail sent to government agencies.

Communication with Politicians (Table 12) Unlike mail on official business, respondents felt that neither newsletters from politicians nor mail to political leaders required any kind of special protection. Once again this is somewhat surprising, given that such communications are easily spoofed either to discredit a politician or to mislead leaders about the depth of public support on a particular issue.

There was no statistically-significant difference between the way that any of our groups answered this question, so individual breakdowns by group are not provided.

3.3 Opinions of Companies That Send Digitally-Signed Mail (Table 13)

When queried on a scale of 1 to 5, where 1 was "Strongly Agree" and 5 was "Strongly Disagree," respondents on average slightly agreed with the statement that companies sending digitally-signed mail "Are more likely to have good return policies." Respondents also slightly agreed with the statement that such companies "Are more likely to

Table 11. Financial Communications: What Kind of Protection is Necessary?

	"A bank or credit-card statement:"	"Mail to government agencies on official business, such as filing your tax return or filing complaints with regulators:"
Does not need special protection	1.2%	4.2%
Should be *digitally-signed*	2.1%	9.2%
Should be *sealed* with encryption	16.2%	9.9%
Should be *both* signed and sealed	62.7%	64.6%
Should never be sent by email	17.8%	12.2%
sealed or *both*	78.9%	74.4%
digitally-signed or *both*	64.8%	73.7%
Total Respondents	426	426
No Response	(7)	(7)

Table 12. Communication to and from Political Leaders: What Kind of Protection is Necessary?

	"Newsletters from politicians:"	"Mail to political leaders voicing your opinion on a matter:"
Does not need special protection	54.9%	52.5%
Should be *digitally-signed*	19.7%	27.2%
Should be *sealed* with encryption	0.5%	4.2%
Should be *both* signed and sealed	2.1%	10.3%
Should never be sent by email	22.8%	5.9%
sealed or *both*	2.6%	14.5%
digitally-signed or *both*	21.8%	37.5%
Total Respondents	426	427
No Response	(7)	(6)

be law-abiding." No significant difference was seen between any of our groups for these two questions.

We were curious as to whether or not interest in cryptography was seen as an American technology, so we asked respondents whether or not they thought that companies sending digitally-signed mail "Are more likely to be based in the United States." Interestingly enough, this *did* have statistically-significant variation between our various groups. The *Europe* and *Savvy* groups disagreed with this statement somewhat, while the *US* and *Green* groups agreed with the statement somewhat.

When asked whether or not a digitally-signed message "is more likely to contain information that is truthful," respondents neither agreed nor disagreed, with no significant difference between our four groups.

All groups disagreed somewhat with the statement that digitally-signed mail "is less likely to be read by others," although respondents in the *Europe* group disagreed with the statement significantly more than the *US* group.

Table 13. Do you *strongly agree (1)* or *strongly disagree (5)* with the following statements?"

Companies that send digitally-signed mail

Question	Group	$\overline{x}$	n	σ
"Are more likely to have good return policies"	ALL	3.0	412	1.07
"Are more likely to be law-abiding"	ALL	2.8	412	1.17
"Are more likely to be based in the United States"	**Europe**	**3.5**	77	1.28
	US	**3.0**	334	1.13
	Savvy	**3.3**	135	1.26
	Green	**3.0**	276	1.12

Digitally-signed mail:

Question	Group	$\overline{x}$	n	σ
"Is more likely to contain information that is truthful,"	ALL	3.0	411	1.20
"Is less likely to be read by others,"	**Europe**	**3.7**	77	1.25
	US	**3.2**	335	1.22

3.4 Free-Format Responses

Our survey contained many places where respondents could give free-format responses. Many wrote that they wished they knew more about email security. For example:

> *I wish I knew more about digitally-signed and sealed encrypted e-mail, and I wish information were more generally available and presented in a manner that is clear to those who aren't computer scientists or engineers.*
>
> *This is an interesting topic... I had not thought about the need to send/receive signed or sealed e-mail for other than tax info.*

Others do not understand cryptography and do not want to learn:

> *Most sellers do not care about digital signatures when selling on on-line marketplaces unless they are dealing in big sums of money in the transaction, even then I still do not care.*
>
> *I think it's a good idea, but I'm lazy and it's too much trouble to bother with.*

These comments, and many others, reinforce our belief that the usability standards for a successfully-deployed email security system must be extraordinarily high. It is not enough for systems to be easily learned or used, as Whitten argues. [13] Instead, we believe that normal use of security systems must require zero training and zero keystrokes. Security information should be conveyed passively, providing more information on demand, but should not otherwise impact on standard operations.

Many respondents used the free-format response sections to complain about spam, viruses, and phishing — sometimes to the point of chastising us for not working on these problems:

> *I hope this [survey] will help to stop the viruses, spam, spyware and hijackers all too prevalent on the web.*

> *[I] feel the topic is somehow "phony" because of the way viruses are transmitted by email. I'm more concerned with attacks by future NIMDAs*[4] *than I am with sending or receiving signed email.*

Several respondents noted that there is little need to send sealed email, since such messages can be sent securely using feedback forms on SSL-encrypted websites.

4 Conclusions and Policy Implications

We surveyed hundreds of people actively involved in the business of e-commerce as to their views on and experience with digitally-signed email. Although they had not received prior notification of the fact, some of these individuals had been receiving digitally-signed email for more than a year. To the best of our knowledge this is the first survey of its kind.

It is widely believed that people will not use cryptographic techniques to protect email unless it is extraordinarily easy to use. We showed that even relatively unsophisticated computer users who do not send digitally-signed mail nevertheless believe that it should be used to protect the email that they themselves are sending (and to a lesser extent, receiving as well).

We believe that digitally-signed mail could provide some measure of defense against phishing attacks. Because attackers may try to obtain certificates for typo or copycat names, we suggest that email clients should indicate the difference between a certificate that had been received many times and one that is being received for the first time—much in the way that programs implementing the popular SSH protocol [15] alert users when a host key has changed.

We found that the majority (58.5%) of respondents did not know whether or not the program that they used to read their mail handled encryption, even though the vast majority (81.1%) use such mail clients. Given this case, companies that survey their customers as to whether or not the customers have encryption-capable mail readers are likely to yield erroneous results.

We learned that digitally-signed mail tends to increase the recipient's trust in the email infrastructure. We learned that despite more than a decade of confusion over multiple standards for secure email, there are now few if any usability barriers to receiving mail that's digitally-signed with S/MIME signatures using established CAs.

Finally, we found that people with no obvious interest in selling or otherwise promoting cryptographic technology believe that many email messages sent today without protection should be either digitally-signed, sealed with encryption, or both.

[4] W32/Nimda was an email worm that was released in September 2001 and affected large parts of the Internet. [14]

The complete survey text with simple tabulations of every question and all respondent comments for which permission was given to quote is at `http://www.simson.net/smime-survey.html`.

4.1 Recommendations

We believe that financial organizations, retailers, and other entities doing business on the Internet should immediately adopt the practice of digitally-signing their mail to customers with S/MIME signatures using a certificate signed by a widely-published CA such as VeriSign. Software for processing such messages is widely deployed. As one of our respondents who identified himself as "a very sophisticated computer user" wrote:

> *I use PGP, but in the several years since I have installed it I have never used it for encrypting email, or sending signed email. I have received and verified signed email from my ISP. I have never received signed email from any other source (including banks, paypal, etc, which are the organisations I would have thought would have gained most from its use).*

Given that support for S/MIME signatures is now widely deployed, we also believe that existing mail clients and webmail systems that do not recognize S/MIME-signed mail should be modified to do so. Our research shows that there is significant value for users in being able to verify signatures on signed email, even without the ability to respond to these messages with mail that is signed or sealed.

We also believe that existing systems should be more lenient with mail that is digitally-signed but which fails some sort of security check. For example, Microsoft Outlook and Outlook Express give a warning if a message is signed with a certificate that has expired, or if a certificate is signed by a CA that is not trusted. We believe that such warnings only confuse most users; more useful would be a warning that indicates when there is a change in the distinguished name of a correspondent—or even when the sender's signing key changes—indicating a possible phishing attack.

4.2 Future Work

Given the importance of email security, a survey such as this one should be repeated with a larger sample and a refined set of questions.[5] It would also be useful to show respondents screen shots of email that was digitally-signed but which failed to verify (for example, because the message contents had been altered or because the CA was created by hackers for a phishing website) and ask what they would do upon receiving such a message. Organizations interested in sending digitally-signed mail may wish to consider before-and-after surveys to gauge the impact of the mail signing on those receiving the messages

[5] In particular, no questions were asked on the subject of medical privacy.

5 Acknowledgements

The idea for survey was originally suggested by Jean Camp when she was at Harvard's Kennedy School. Sean Smith at Dartmouth College, John Linn at RSA Security provided useful comments. We are thankful to David C. Clark, Karen Solins and Min Wu for their initial comments on our survey questions, and to Steven Bauer, David C. Clark, David Krikorian and Sian Gramates for their comments on the final paper. John-Paul Ferguson at MIT and Elaine Newton at CMU provided useful comments on our statistical methods. Amazon.com's computer security group and nearly 200 other Amazon employees graciously pretested an earlier version of this survey. Apart from allowing its employees to participate in the study, Amazon.com did not contribute monetarily to this study and does not necessarily endorse the conclusions and recommendations herein.

References

1. Gutmann, P.: Why isn't the internet secure yet, dammit. In: AusCERT Asia Pacific Information Technology Security Conference 2004; Computer Security: Are we there yet? (2004) http://conference.auscert.org.au/conf2004/.
2. Federal Trade Comission: Identity thief goes "phishing" for consumers' credit information (2003) http://www.ftc.gov/opa/2003/07/phishing.htm.
3. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: 8th USENIX Security Symposium. (1999) 169 – 184
4. Linn, J.: RFC 989: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures (1987) Obsoleted by RFC1040, RFC1113 [5, 6]. Status: UNKNOWN.
5. Linn, J.: RFC 1040: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures (1988) Obsoleted by RFC1113 [6]. Obsoletes RFC0989 [4]. Status: UNKNOWN.
6. Linn, J.: RFC 1113: Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures (1989) Obsoleted by RFC1421 [16]. Obsoletes RFC0989, RFC1040 [4, 5]. Status: HISTORIC.
7. Zimmermann, P.R.: The Official PGP User's Guide. MIT Press (1995)
8. Atkins, D., Stallings, W., Zimmermann, P.: RFC 1991: PGP message exchange formats (1996) Status: INFORMATIONAL.
9. Elkins, M.: RFC 2015: MIME security with pretty good privacy (PGP) (1996) Status: PROPOSED STANDARD.
10. Dusse, S., Hoffman, P., Ramsdell, B., Lundblade, L., Repka, L.: RFC 2311: S/MIME version 2 message specification (1998) Status: INFORMATIONAL.
11. Ramsdell, B.: Secure/multipurpose internet mail extensions (s/mime) version 3.1 message specification (2004)
12. GVU: GVU's tenth WWW user survey results (1999) http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/.
13. Whitten, A.: Making Security Usable. PhD thesis, School of Computer Science, Carnegie Mellon University (2004)
14. CERT Coordination Center: CERT advisory ca-2001-26 nimda worm. Technical report, CERT Coordination Center, Pittsburgh, PA (2001)
15. T. Ylonen, e.a.: SSH protocol architecture (1998) Work in Progress.
16. Linn, J.: RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures (1993) Obsoletes RFC1113 [6]. Status: PROPOSED STANDARD.