

# **THE LANGUAGE OF SCAM SPAMS: LINGUISTIC FEATURES OF “NIGERIAN FRAUD” E-MAILS**

DEBORAH SCHAFFER

*This article examines the general nature, history, and language features of one type of fraudulent e-mail spam, the ubiquitous Nigerian fraud (4-1-9) letter. Patterns in content include similar narratives involving vast sums of money to be transferred from the scammer's home country with outside help and common persuasive strategies frequently involving apologies, flattery, attempts to intrigue recipients, and appeals to greed, altruism, trust, and religious feelings, while patterns in writing features include use of attention-inducing buzz words like “urgent” and “secret” in subject headings as well as in the letters themselves, and obvious nonnative English grammar, mechanics, and vocabulary errors. In spite of the cruder elements of these letters and worldwide efforts to fight the con artists sending them, recipients are still drawn in to these scams in large numbers, losing millions of dollars every year. The best defense against them must still entail comprehensive public education about the nature of this scam (and others) and about the telltale characteristics of these letters that signal a con at work.*

---

Deborah Schaffer received her PhD in linguistics from The Ohio State University and is currently a professor of English at Montana State University Billings, where she teaches linguistics, composition, and genre literature. She was the chair of the Language Attitudes and Popular Linguistics Area of the Popular Culture Association from 1991 to 2005 and has had her research published in the anthology *Barbarians at the Gate: Studies in Language Attitudes*, as well as in *The Journal of Pragmatics*, *English Today*, *ETC.*, *The Journal of Popular Culture*, *The Journal of Phonetics*, and other venues. An earlier version of this paper was presented at the 34th Annual Popular Culture Association Conference, San Antonio, April 7–10, 2004.

## Introduction

Just as junk mail appears to be the price of an effective postal service, so unsolicited commercial e-mails (UCEs for short; see Holt and Berg, 2002) or “unsolicited bulk e-mails” (Gleick, 2003, p. 16)—more popularly known as spam—seem to be the price of an open electronic communications system. According to James Gleick (2003, p. 16), the first spam has been identified as a product blurb sent by a Digital Equipment Corporation employee in 1978 to hundreds of participants on the Arpanet—all of whose addresses were typed by hand. The real spam boom, Gleick says, didn’t start until 1993 or 1994 (2003, p. 16), but since then, as we all know, the increase in spamming has been astronomical. By June 2003, it was estimated to make up “49% of network traffic” (Woellert, 2003, p. 54), amounting to 15 billion e-mails a day in December 2003 (Baker, 2003, p. 78), and by 2008, according to David Pye, spam added up to “anywhere from 75% to 90% of all global e-mail traffic” (2008, p. 20), or “close to 100 billion spam messages ... transmitted worldwide daily” (2008, p. 20). Along with advertising spams, even more unfortunately, have come outright fraudulent e-mails. Alan Goldstein reports that in June 2002, scam e-mails comprised 6% of total spam mailings (2002, p. D10), with such frauds already bilking individuals and companies out of seven to eight billion dollars a year in 2001 (York, 2001, p. 8), while Mitch Lipka claims that complaints to the Internet Crime Complaint Center increased by 33% from 2007 to 2008, citing losses for the latter year at 265 million dollars (2009, p. 2).

A more recent wrinkle (first seen in March 2003, according to “SurfControl Reminds Companies,” 2002) involves “brand spoofing” (aka “phishing”; see, for example, Emling [2003, p. C1] and “Gone Phishing” [2004, p. 91]), where e-mails designed to look like legitimate mailings from reputable businesses con recipients into disclosing to a Web site personal financial information, like bank-account numbers, passwords, and social-security numbers, that is then used to steal victims’ money or even identities (“SurfControl Reminds Companies,” 2002). And now “pharming,” “a far less detectable form of phishing” (Pye, 2008, p. 20), actually corrupts users’ computers through the surreptitious installation of malware that hijacks the unsuspecting typer of true site addresses to fake but legitimate-looking sites where personal information can also be stolen from the unwary.

But long before these scams, and in addition to the Internet-based versions of the usual nonelectronic forms of fraud involving nonexistent or nonperforming products, there have appeared in countless in-boxes various

fraudulent spams offering a chance at big rewards for minimal effort. This category may involve variations on the pyramid scheme or chain letter; announcements that the recipient has won a lottery or other prize, which turns out to cost some money to claim; and some version of what is variously known as “Nigerian spam” (Gleick, 2003, p. 16), “‘Nigerian letter’ fraud” (Goldstein, 2003), “advance-fee fraud” (Cruickshank, 2001, p. 1; Mikkelson, 2003; Schronen, 2004; United States Secret Service, 2002), or Nigerian “4-1-9 fraud” or “419 scam,” after the section in Nigeria’s penal code that deals with fraud, according to Norr (2002, p. A6) (see also Brady [2003, p. 1], Dupin [2003, p. 24], and Schiesel [2004, p. G1]). Many other sources also discuss this category of fraud, including two books on the subject, one by Harold Baines (1996) and one by Charles Tive (2002), and several law-enforcement and other Web sites, including those of the Bureau of International Narcotics and Law Enforcement Affairs of the United States Department of State, the Federal Trade Commission, The 419 Coalition, The Freeman Institute, and the United States Secret Service.

Brendan Koerner (2002) and Barbara Mikkelson (2003) both trace this scam’s roots back to the 1920s “Spanish Prisoner” con in which victims are duped into sending more and more money to help obtain the release of a wealthy family’s relative imprisoned in Spain (who, of course, does not exist) in hopes of being well rewarded (which, of course, they never are). The current Nigerian version, according to Koerner (2002), first took the form of mailed photocopies in the late 1970s, continuing, as Gavin McCormick (2002) says (see also Brady [2003, p. 1] and Norr [2002, p. A6]), as print letters in the 1980s and faxes in part of the 1990s, but popularized even more by the Internet’s ability to reach millions of targets all over the world very cheaply. In 2001, it was the “fastest growing online scam,” according to Henry Norr’s source, Internet Fraud Watch (2002, p. A6), increasing 900% from 2000 to 2001 alone (Denes, 2002, p. 8; Koerner, 2002) and comprising 15.5% of all complaints sent to the Internet Fraud Complaint Center in 2001 (Goldstein, 2002, p. D10) and 4% of total Internet-based fraud in 2002 (Brady, 2003, p. 1), but down to 2.8% of reported electronic fraud in 2008 (“Nigeria,” 2009).

The typical e-version of this letter (see many accounts, including Blommaert and Omoniyi’s genre analysis [2006, pp. 581–83+], Brady [2003, p. 1], Cruickshank [2001, p. 1–2], Dupin [2003, p. 24], Ellis [2003, p. 6], Husted [2002, p. 3F], Lambeth [2002, p. 29], McCormick [2002], Mikkelson [2003], Norr [2002, p. A6], and United States Secret Service [2002]) is sent by someone claiming to be a Nigerian official or other important public figure.

He or she claims to have access to millions of dollars, often obtained illegally, and offers to give the recipient of the letter some percentage of the loot for helping move the money to an account in another country. Should curious recipients reply to the initial e-mail, they receive further urgent messages containing more persuasive rhetoric reinforcing the lure of supposedly easy wealth and with short deadlines meant to deny them thinking time, plus confidentiality conditions meant to prevent them from hearing skeptical second opinions. They are also pressured to phone the scammers (where saying no can be even harder, and the victim ends up paying exorbitant phone bills, according to The Freeman Institute, 2005), may receive impressively authentic-looking government or financial documents (The Freeman Institute, 2005; United States Secret Service, 2002), and so in many cases get persuaded by greed and reassurances of legitimacy into signing on to the deal.

However, to participate, the recipients must at the least send to the "official" some personal contact information (like phone or fax numbers, e-mail address, etc.), plus bank-account and other financial data and possibly even business cards (Norr, 2002, p. A6) and blank business letterhead on which scam-supporting letters will be forged and sent to other possible victims (United States Secret Service, 2002), often along with initial payments supposedly for transfer fees, taxes, or other bogus expenses. Besides keeping whatever money is actually sent, the scammers may also empty any financial holdings the recipients have made vulnerable through disclosure of their personal information, but more often, the goal is rather to confirm that the targets are fully sucked in so that they will keep sending money voluntarily to help the scheme overcome the obstacles, like extra fees, unexpected bribes, etc., which, of course, keep coming up (Cruickshank, 2001, p. 2; United States Secret Service, 2002). Frequently, too, the victims are lured abroad, where "there are language problems ... and they feel less comfortable and are more at risk" from the scammers and other criminals (Ellis, 2003, p. 6), who may have brought them in illegally so as to have more control over them and who may turn their encounters into straight kidnappings for ransom or even murder (see The Freeman Institute [2005], "'Nigerian' Scam" [2003], Riga [2003, p. B1], United States Secret Service [2002], and others).

Koerner (2002) claims that the United States Secret Service estimated the yearly take from this scam as of 2002 at \$100 million, while Norr (2002, p. A6) says that the average cost per victim for 2001 was \$5,957, almost twice that for 2000 and much more than for other forms of fraud (e.g., auction fraud), but also much more than the \$1,650 per complainant reported to the Internet Crime Complaint Center in 2008 (Lipka, 2009, p. 2).

Regardless of the variability of these statistics, this particular scam clearly remains popular with cyber criminals and continues to be a danger for the unwary.

The first Nigerian scam letter I received came to my inbox in March 2002; since then, dozens more have appeared, sometimes in spates of two to four a day, and one (from an ostensible Libyan general) as recently as July 2011, though the rate slowed after 2004. I eventually collected enough of these e-mails to realize that interesting linguistic similarities could be recognized among the samples I had amassed, suggesting that a thorough examination of the language used in these letters could shed light on the scammers' linguistic background, strategies, and goals and perhaps, given their ubiquity and success rate, also reveal broader cultural implications both for senders, many of whom *are* Nigerian or live in various developing countries with both economic problems and opportunities, and for recipients, most of whom live in the United States and other rich, developed countries in the West.

Some features of Nigerian fraud letters, including language characteristics, have already been pointed out in published articles. The largest study is Blommaert and Omoniyi's (2006) analysis of types of competence—technological, cultural, *and* linguistic—demonstrated in these e-mails. They identify a number of common language features, mostly narrative strategies and other content (e.g., introductory apologies and reassurances of confidentiality) but also including grammar and mechanics features, some of which have also been remarked on briefly by other researchers (including Riga [2003, p. B1], Koerner [2002], and Norr [2002, p. A6]).

A number of other print and online publications have also summarized and discussed the narratives and persuasive strategies found in typical 419 e-mails (see many sources cited earlier, especially The Freeman Institute [2005] and United States Secret Service [2002]). Douglas Cruickshank (2001, p. 1), in particular, laments that “the literary merit of the letters themselves is rarely discussed” and proceeds to wax lyrical about the dramatic storylines (the “earnest, alluring evocations of dark deeds and urgent needs”) and the “lavishly stilted prose excavated from an eighteenth century protocol handbook” that he argues “is as awkward and archaic as it is enchanting.” He also praises the “poetic sweetness” (p. 1) of the openings; the persuasiveness of details provided about the senders, money sources, and other elements of the plots (pp. 2–3); and the use of impressive vocabulary, e.g., “modalities” (p. 3). In addition, Norr cites typical subject headings such as “Confidential – mutual benefit” and “Very urgent business proposal” (2002, p. A6).

On the grammar side, Chris Dupin characterizes many of these fraudulent e-mails as “written in broken English” (2003, p. 24), Norr labels the letters’ writing style as “simultaneously pompous, ingratiating and ungrammatical” (2002, p. A6), and Blommaert and Omoniyi point out that “many of the authors of the messages struggle with basic literacy skills and have an incomplete control over standard varieties of English” (2006, pp. 598–99).

All these characteristics can also be observed in my sample, but additional features are also quite common, as a more detailed analysis of the specific language used in these e-mails reveals.

### Procedure

My database consists of 30 e-mailed letters received between March 28, 2002, and July 29, 2003. While I also received other obvious scam letters during and after this time, I included in this study only those which followed the basic outlines of the Nigerian letter fraud, as described earlier, and restricted the sample size to make detailed analysis of the e-mails’ language and content manageable.

I then read through each letter; noted background information on sender and plan details; and analyzed the language used, including narrative content and structure, vocabulary, persuasive techniques, and errors in written English. The highlights of this analysis are presented in Table I.

### Analysis

#### *Country of Origin*

First, I found that 50% of senders claimed to be located in Nigeria; nine other purported countries of origin included the Ivory Coast (13.3%), South Africa (6.7%), the United Arab Emirates (6.7%), Benin (6.7%), and five others responsible for one e-mail apiece (3.3%)—Zimbabwe, Sierra Leone, Kuwait, Togo (typed as “Lome-Togo”), and Guinea-Bissau (typed as “Guinee Bissau”). Thus, only half of the e-mails in my corpus were true *Nigerian* fraud letters (assuming senders’ country identifications were accurate), while the rest came predominantly but not exclusively from other countries in Africa; this was still, however, a greater proportion than the roughly 20% Blommaert and Omoniyi found in their corpus (2006, p. 584).

#### *Senders and Addressees*

Only 40% of the letters came actually addressed to the *recipient*; 53.3% were addressed to the *sender’s own e-mail* (or in one case, the sender’s name), while 6.7% were sent to e-mails *different from the senders’*, and one (3.3%)

**Table I.** Distribution of Major E-mail Language Features

<i>Feature</i>	<i>No. of E-mails (n = 30)</i>	<i>Percentage</i>	<i>Feature</i>	<i>No. of E-mails (n = 30)</i>	<i>Percentage</i>	<i>Feature</i>	<i>No. of E-mails (n = 30)</i>	<i>Percentage</i>
Nigerian Origin	15	50.0	"Reply" or "Response" in Subject Heading	5	16.7	First & Second Person	30	100.0
Ivory Coast Origin	4	13.3	"Dear" in Salutation	18	60.0	Conciliatory Opening	14	46.7
Addressed to Sender's Own E-mail	16	53.3	"Attention" in Salutation	7	23.3	Unexpected Nature of E-mail	7	23.3
Addressed to Recipient	12	40.0	Salutation	16	53.3	E-mailer's Link to Recipient	11	36.7
"Urgent" in Subject Heading	10	33.3	Response Urged in Closing	15	50.0	Religious Appeal	7	23.3
"Business" in Subject Heading	5	16.7	"(Best) Regards" in Closing	10	33.3	Secrecy Appeal	25	83.3
"Please" in Subject Heading	5	16.7	"Yours" in Closing	9	30.0	Urgency Appeal	22	73.3
"Assist/ance" or "Help" in Subject Heading	5	16.7	Urgency in Closing	7	23.3	Business Representation	18	60.0
			Thanks in Closing	4	13.3	Safety Appeal	15	50.0
			Cooperation Reference in Closing			Benefit Appeal	10	33.3

(Continued)

Table I. Distribution of Major E-mail Language Features (Continued)

Feature	No. of E-mails (n = 30)	Per- centage	Feature	No. of E-mails (n = 30)	Per- centage
Comma Errors	28	93.3	Sg./Pl. Problems	24	80.0
Other Punctuation Errors	28	93.3	Word-Form Problems	21	70.0
Missing Words	26	86.7	Spelling Problems	17	56.7
Capitalization Problems	25	83.3	Agreement Problems	13	43.3
Word-Choice Problems	25	83.3	Awkward Phrasing	12	40.0
Sentence-Structure Errors	24	80.0	Tense Problems	10	33.3
			Learned/Specialized Vocabulary	28	93.3

Other features found in 10% or fewer of e-mails in corpus: other countries of origin (South Africa, United Arab Emirates, Benin, Zimbabwe, Sierra Leone, Kuwait, "Lome-Togo," "Guinee Bissau"); other words in subject heading ("proposal/proposition," "personal," "relationship"); other words in salutations ("Sir," "Good Day," "Greetings," "Hello," "From:"); other strategies in closings (references to God or Christ, references to confidentiality); wordiness/extra words; typed all in capital letters.



was addressed to a *totally different (and unknown) name*. And scam spams appear to be a man's game (as The Freeman Institute [2005] also points out): only 16.7% were putatively sent by *women* (among them, one "Lady," a "Miss," and two "Mrs."), leaving 83.3% sent by men. Thirty percent were sent by self-designated *doctors* (all men), with four others sent by one "Auditor," one "Barrister," one "Brigadier-General," and one "ENGR". The rest (female or male) offered no titles.

### *Subject Headings*

The *subject headings* varied considerably, but certain key words occurred fairly frequently (some together in the same heading):

- "urgent" (in 33.3%);
- "business" (16.7%);
- "please" (16.7%);
- "assist," "assistance," or "help" (16.7%);
- "reply" or "response" (16.7%); and
- "proposal" or "proposition" (10%).

Norr's (2002, p. A6) heading findings are thus at least partly duplicated in my sample, "urgent" and "business" appearing frequently in both heading samples, while Norr's additional key words "confidential" and "benefit" are also actually common in the bodies of my e-mails, though not in the subject headings. Likewise, Blommaert and Omoniyi's characterization of the majority of their e-mails' subject headings as "seek[ing] *personal rapport and involvement in style*" (2006, p. 589; italics original) can be argued to apply to my sample, as well.

### *Salutations*

The *salutations* also frequently employed the same words (and these words also appear in Blommaert and Omoniyi's (2006) samples, along with additional openings; see page 590):

- "Dear" was used in 60% of the e-mails: "dear sir" headed 30%; "dear friend" headed 13.3%, "dear madam" headed one (3.3%); and "dear," "my dear," or "dearest," with no title or other form of address, headed 13.3%;
- "ATTN," "Attention," or "your attention" headed 23.3% of e-mails; and
- "Good day" headed 10%.

### Closings

The *closings* also showed considerable variety but again offered some patterns, often in combination (see also the example cited in Blommaert and Omoniyi [2006, p. 589]):

- 53.3% requested or urged a *response* in some form (as in “Your immediate response will be highly appreciated”);
- “Best regards” or “regards” ended half of the e-mails;
- “Yours,” either alone or in combination with “Sincerely,” “Truly,” “Faithfully,” or—in one case—“Yours in Christ,” ended 33.3%;
- 30% stressed the *urgency or immediacy* of the proposal or hoped-for reply (as in “I waiting [sic] to hear from you soon”);
- 23.3% closed with some form of *thanks*;
- 13.3% indicated *expectations of cooperation or collaboration* (as in “Thank you in advance for your anticipated co-operation”); and
- 10% closed with references to *God* or *Christ* (“Yours in Christ”; “Cheers and God bless you”; “God be with you”).

### Narratives

As for *narrative content*, first, there was some variety in the stories told, but within the same general narrative frame described earlier, and of the type referred to by Erving Goffman (1974, p. 103) and others as “exploitive fabrication[s]”: individuals of different backgrounds claimed to have access to millions of dollars and offered to give the recipient of the letter some percentage of the wealth for helping dispose of the money in some advantageous way. However, of the seven plot outlines noted by the United States Secret Service (2002), only two appeared in my corpus: “contract fraud,” and “transfer of funds from over invoiced [sic] contracts” (leaving the “beneficiary of a will,” “recipient of an award,” “purchase of real estate,” “conversion of hard currency,” and “sale of crude oil at below market prices” plots unrepresented). Likewise, of the five scam categories described by The Freeman Institute (2005), only the “Contract Repurchase 419” (buying another firm’s contract earnings) and “Charity Scam 419” (helping persecuted people get their wealth out of the country) seem to apply (with greater or lesser fidelity) to the letters I examined, while “Oil 419” (a Nigerian oil deal), “Black Currency 419” (buying chemicals to clean money), and “Will Scam 419” (obtaining money left to the scam victim in a will, rather than helping to carry out the deceased’s wishes) do not. Finally, of Blommaert and Omoniyi’s four

categories of stories, “dormant accounts” (2006, p. 581), “lottery rewards” (2006, p. 581), “rescue operations” (2006, p. 582), and “charity” (2006, p. 583), all but the lottery plot are represented in my corpus, as well (like Blommaert and Omoniyi, I see lottery offers as belonging to a different genre of fraud letters from the others and so chose to omit them from this analysis).

In my collected e-mails, specifically,

- 30% claimed to come from *government officials* who had illegally diverted money to invest abroad;
- 30% were sent by a *dead millionaire’s relative, representative or lawyer* to request help in transferring the deceased’s estate out of the country;
- 16.7% were pleas from *bank officials* wishing to divert the contents of a dead customer’s account to the e-mail recipients’;
- 6.7% were from a *business executive* who had illegally diverted money to invest abroad (so a variation on the first story line);
- 6.7% were sent by *dying millionaires* needing outside help to dispose of their wealth in some socially beneficial way;
- 6.7% came from *supposedly legitimate business people* seeking a business partner abroad who could facilitate safe foreign investments; and
- One (3.3%) sought a partner outside the sender’s country to *help access a foreign account*.

In general, all the writers but one introduced themselves early in the letter, providing their backgrounds and how they came to have access to the money, and all but one explained the crisis or other development that led to the need for outside help before explaining to at least some extent the recipient’s hoped-for role in the transaction and what his/her reward would be (mentioned in 90% of the e-mails in greater or lesser detail), sometimes (in 46.7% of all e-mails) within a larger breakdown of percentages for everyone involved (e.g., “17% for your assistance ... 80% for myself & my Colleagues ... 3% for contingency expenses”). Most then ended with a request for a response, often to be accompanied by some contact information. No letter asked for money at any point or indicated that future expenses might be involved.

### *Persuasive Strategies*

There were also some recurring themes within the individual persuasive strategies used by the scammers. First, and hardly surprisingly, all 30 e-mailers (100%) used both *first* and *second person* in providing their own personal

stories and appealing directly to the recipient. But in addition, about half tried to *ingratiate* themselves with the recipient in different ways:

- 46.7% opened their letters with *conciliatory* or *apologetic* comments, as also noted by Blommaert and Omoniyi (2006, pp. 590–91) (e.g., “Compliments of the season, and I pray that this mail meet you in good Health.” and “Pardon the abruptness of this letter; it is due to its exigency.”), clear examples of negative politeness used to signal the senders’ desire not to impose on the recipient (see Brown and Levinson [1987, p. 70]);
- 23.3% specifically *acknowledged the unexpected nature of the e-mail* (e.g., “I know this proposal letter may come to you as a surprise considering the fact that we have not had any formal acquaintance before.”);
- 36.7% offered information on *how the recipient came to their attention*, with or without some *flattery*—also mentioned by The Freeman Institute (2005)—attached (e.g., “You have been recommended by an associate who assured me in confidence of your ability and reliability in prosecuting a business transaction of high net value requiring maximum confidentiality.”); and
- 23.3% tried *religious appeals*, also reported by The Freeman Institute (2005) (either invoking God, as in “Thanks and God bless” in one closing, or otherwise displaying the sender’s religious faith, as in one letter’s quoting a passage from Exodus—14:14: “the lord will fight my case and I shall hold my peace [sic]”).

Another tack scammers took involved attempts to *intrigue recipients* (perhaps invoking Jib Fowles’ advertising appeal to the basic need to satisfy curiosity [1982, p. 286]) or *spur them into action*:

- 83.3% proclaimed the *confidentiality* or *secrecy* of their business, as Blommaert and Omoniyi (2006, pp. 596–97), The Freeman Institute (2005) and the United States Secret Service (2002) also point out (as in “First, I must solicit your strictest confidence in this transaction; this is by virtue of its nature as being utterly confidential and top secret.”); and
- 73.3% of e-mails stressed the *urgency* or *immediacy* of their message, also reported by The Freeman Institute (2005), the United States Secret Service (2002), and others (as in “As I expect your urgent reply.” in the closing of one e-mail, and “Get Back To Me Urgently!” in another’s subject heading).

And, of course, a large number of scammers tried different sorts of *appeals* to *various needs* or *desires* of the recipients:

- 60% clearly tried to *legitimize their scams* by referring to them as business proposals, propositions, relationships, and transactions (as in “My primary reason for writing to you is to seek your partnership/ assistance in a business transaction.”);
- 50% promised that their dealings would be *safe*, as also reported by The Freeman Institute (2005) and fitting Fowles’ appeal to the need to feel safe (1982, p. 285) (as in “This transaction is 100% risk free.” and “This project is not risky.”); and
- 33.3% touted the *benefit, profit, or value* to accrue to the e-mail recipient if s/he agreed to participate, in keeping with Fowles’ appeal to the need to achieve (1982, p. 282) (e.g., “The reason for this letter is that your help is being sought in order to ... successfully complete a profitable venture that is of immense benefit to you ...”).

### Grammar

Unsurprisingly, and in keeping with Blommaert and Omoniyi’s (2006, pp. 599–603), Dupin’s (2003, p. 24), and Riga’s (2003, p. B1) characterizations, the majority of these scam mailings were easily identifiable as having been written by *nonnative speakers of English* (ESL speakers). In fact, only 20% demonstrated real fluency, while the rest offered a variety of *grammatical and mechanical infelicities* (some also frequently found in native English writings, but many clearly the product of incomplete mastery of the language), as well as *malapropisms* and *garbled syntax*:

- 93.3% of the letters contained *comma errors* (either missing or unneeded commas);
- a slightly different 93.3% contained *other punctuation errors* (everything from missing or misused apostrophes to period, quotation-mark, and colon problems);
- 86.7% were clearly *missing words* in at least one sentence (as in “I have all necessary formation [sic] and legal documents needed to back you up for claim.”);
- 83.3% had *capitalization problems* (either misused or missing capitals), although only 10% were typed exclusively in capitals (counter to Norr’s [2002, p. A6] observation of greater frequency but in keeping

with Blommaert and Omoniyi's finding of "unwarranted use of capitals" [2006, p. 599]);

- another 83.3% had *word-choice problems* (that is, clearly wrong words were used, as in "I meant ... to pass a very urgent and profitable Business proposal and *well approaching matter across* to you.");
- 80% contained at least one *sentence-structure error*: 50% contained *comma splices*, 46.7% contained *fragments*, and 30% contained *run-ons*;
- another 80% had *incorrect uses of singular or plural word forms* (as in "my Lawyer will make *preparation* for my family to come over to your country.");
- 70% had *word-form problems* (as in "I *wait* your urgent *respond* immediately.");
- 56.7% contained *misspelled words* (even with spell check);
- 43.3% had *subject-verb and/or pronoun-antecedent agreement problems*;
- 40% had *awkward phrasing* not involving misused words (as in "Please send to me your ... fax number where the Certificate of Deposit ... will be fax to you *for the claiming of the consignment*."); and
- 33.3% had *tense problems* (as in "Sir my message to you *was* based on ...").

### Diction

Looking more closely at the kinds of word-choice problems evident in these e-mails, one finds not only *low-level mistakes* like *incorrect prepositions* (as in "and he died, *since* 1993") and *articles* (as in "I seek *the* consent to present you as the next of kin to the deceased") that clearly mark ESL speakers, but also a number of bona fide *malapropisms* (e.g., "I pray that this mail *meet* you in good Health" for *finds*; and "the will to *personify the façade* to its practical conclusion" for *pursue the charade*) which are still, however, mostly markers of nonnative competence.

But in addition, 93.3% of these letters also made use of *learned or specialized vocabulary*, quite clearly for effect—i.e., to make their senders sound educated (certainly the Latin terms used on rare occasions, like "bonafide [sic]" and "modus operandi," attest to this) or at least knowledgeable in the military, financial, or other arenas they claim to be involved in. These words *were* mostly used correctly, if not comfortably—as in "the *remittance* of the funds" and "for your *perusal*"—although some were odd enough (at least, perhaps, to American English speakers) to suggest

someone's hopeful idea of what formal English should sound like: consider "so that I can furnish you with further details on the *modalities* of the transfer of the fund into your bank account" (note the use of Cruickshank's [2001] prized word here) and "government officials ... awarded themselves contracts that were grossly over-invoiced in various ministries and *parastatals*." And yet the most fluent letters were in fact quite well written, even confidence-inspiring, for example, "However, if you do [reply], and the conditions are right, you will be amply compensated. It is also pertinent to add that I am using an assumed name"; and "An important client of mine whose details I cannot release at this point has implored me to contact a reliable and trustworthy partner overseas").

### Conclusion

Given the writing characteristics just overviewed, most of these letters appear likely to have been written by minimally competent English speakers who nevertheless are clearly trying to use language that will impress, entice, reassure, and/or evoke sympathy in their readers—hence, the impressive titles and vocabulary used by some senders; the ties to important figures claimed by most of them; the frequent appeals to politeness, safety, legitimacy, secrecy, and urgency; and the tales of injustice, crises, and/or golden opportunities and the promises of great fortunes presented in all these e-mails. If they are aware of their limitations in English—and Blommaert and Omoniyi suggest otherwise, claiming that at least some of these writers "appear to assume that *their English is 'good' enough to pass as native speakers* [sic]" (2006, p. 602; italics original)—I suspect they count on the content of their mailings to prove irresistible to recipients, with greed winning out over skepticism.

Is it surprising that so many amateurishly written e-mails are being sent to so many native English speakers, given that we might well assume that any such adult with enough education to be able to use a computer should also be able to see how badly composed and undoubtedly fraudulent these e-mails are? Not when one considers the economics of the situation, specifically, how cheap it is to scatter thousands of spams worldwide and how profitable even a miniscule reply rate will be, especially when in West Africa, for example, as small a score as \$250 can pay the bills for close to a year (The Freeman Institute, 2005). These scammers set up free, anonymous e-mail accounts accessed through cheap cybercafé computers (Koerner, 2002), probably invest minimal time in writing and sending the mailings,

and have very little to lose and potentially a great deal to gain by casting their nets as widely as possible.

Furthermore, where high unemployment means that Nigeria (or anywhere else, for that matter) “teems with bright, underemployed youths” (Koerner, 2002) who are computer literate and have access to both the 419 scheme and the technology to implement it, it seems inevitable that the con would proliferate. In fact, Koerner (2002) claims that “the wiring of Nigeria is being propelled by 419” and predicts that this fraud will decline when “young, educated Nigerians have better economic prospects,” leaving “a thriving Internet culture for Nigerians to use for more legitimate purposes.” In the meantime, however, “mass unemployment, extended family systems, a get rich quick syndrome, and, especially, the greed of foreigners” have encouraged 419 fraudsters and will continue to do so (United States Secret Service, 2002), keeping 419 fraud among the top five industries in Nigeria (Koerner, 2002).

Perhaps, then, on the other side of the con, it should seem more surprising that any literate, computer-competent, native-English-speaking recipient would actually be taken in by these e-mails, a sentiment also expressed by the Federal Trade Commission (“The ‘Nigerian’ Scam” [2003]), The Freeman Institute (2005), Koerner (2002), and others, especially given that “the nonnativeness of their English ... exposes their messages as cases of fraud” (Blommaert and Omoniyi, 2006, p. 602). Of course, as Blommaert and Omoniyi point out, many recipients are themselves *not* native speakers of English and so might not recognize the senders’ lack of English competence (2006, p. 604). But even for fully competent English users, in a country where millions of people buy daily Power Ball tickets, play online lotteries, and make casino owners millionaires, the belief in suddenly striking it rich or otherwise getting something for nothing still obviously holds the American imagination captive. I suspect that most people who take these scam letters seriously are not put off by the poor writing and are quite willing to believe in the various scenarios the scammers set up (especially the ones dependent on all-too-common government or other bureaucratic malfeasance which many Americans probably take to be endemic in Nigeria and many other developing countries). No doubt, they assume that nonnative speakers of English could still have access to riches in their home countries, and perhaps they even take the ESL characteristics of these e-mails as a sign of authenticity, supporting the senders’ claims that they are indeed not American, but citizens of those foreign countries they name. In such a case, a sender’s limited English proficiency would certainly not stand in the way



of making the deal of a lifetime, especially if the recipient's role in the transaction sounds easy, safe, and plausible.

What clearly remains the case is that even today, after all the publicity these e-mails have received, enough scammers must be succeeding at enough of their schemes to keep them sending new pitches out onto the e-waves, as my own inbox can attest. And I suspect that the key to their success lies not in the credibility of their sob stories, and certainly not in the eloquence of their language, but in their promise of a reward too large and too easily earned to be turned down without the recipients' at least learning more about what strings might be attached. And once the marks respond to the e-mail, some of them clearly can be manipulated into actions, from further e-mail correspondence to trips to Nigeria, which cost them big sums (and sometimes put them in grave danger) instead of bringing them easy millions, perhaps due to the same psychological factors at work in "low-balling" tactics used by car dealers and others. In this case, Nigerian fraud letters provide similar opportunities for recipients to become invested (financially and emotionally) in their schemes. Then, as expenses mount (but still add up to only a fraction of the promised reward, as Cruickshank [2001, p. 2] points out) and the payoff recedes, many victims still feel they have too much at stake to cut their losses and walk away.

A number of suggestions have been offered to avoid or reduce spam and protect consumers from fraudulent e-mail schemes, including never responding to spam, refraining from sharing personal information electronically, checking antiscam Web sites, and reporting suspicious e-mails to the Federal Trade Commission or other watchdog groups (see, for example, Bernstein [2009, p. B13], Buechner [2003, pp. 52–3], Dupin [2003, p. 24], Emling [2003, p. C1], Rosenberg [2005, p. A-7], Tive [2002], Valetk [2002, p. s6], Woellert [2003, pp. 54–5], and others). Pye also mentions the growth of security software and defines several computer-based strategies for blocking or screening suspicious e-mails, including "traffic throttling" and "signaturing" (2008, p. 20).

In addition, a few sources have focused specifically on advice for dealing with the Nigerian fraud letter. Among them, The Freeman Institute (2005), Mikkelson (2003), Norr (2002, p. A6), Riga (2003, p. B1) and Schiesel (2004, p. G1) all identify Web sites that variously report news about this type of fraud, provide sample e-mails for viewing, and/or allow people to report cases of fraud to authorities; Dupin (2003, p. 24) and the United States Secret Service (2002) describe several 419 fraud tip-offs and provide Secret Service contact information; Tive (2002) provides a whole chapter on

educating the public and fighting the scam in other ways; and Dudley (2002, p. 1) summarizes explanations and advice available on the nigerianfraud-watch.org site.

But a fairly new course of antifraud action involves “scam baiting” (Riga, 2003, p. B1) or “fraud baiting” (Schiesel, 2004, p. G1). According to Crampton (2007, p. 7), Riga (2003, p. B1), Schiesel (2004, p. G1), Shaw (2007, p. A8), and others, in this approach to fighting e-scams, recipients of Nigerian fraud e-mails respond to the scammers and involve them in various humiliating, time-consuming and hopefully expensive wild-goose chases (e.g., requiring photos of the scammers with ludicrous signs, sending them to far-off cities to collect nonexistent payments, etc.) in an attempt to divert the fraudsters from more gullible marks and, ideally, waste the con artists’ resources. Many also publicize their activities and post correspondence from the scammers on their Web sites (see Crampton [2007, p. 7], Riga [2003, p. B1], and Schiesel [2004, p. G1] for several site addresses, including those for such antifraud groups as Phonebusters, the Anti-419 Coalition, and Artists Against 419).

The spammers, however, are fighting back with a vengeance. On the low-tech side, senders manipulate the content of headers, subject lines, and the letters themselves to make it less obvious that their mailings are spam (Gleick, 2003, p. 16), while higher-tech schemes, as Stephen Baker (2003, p. 82) points out, involve overloading the servers of antis spam organizations with mail in order to shut them down, employing hackers to foil antis spam defenses, and using computer power and viruses to trick spam filters.

Steven Johnson argues that ultimately, the single most effective way to reduce spam will be to make it more expensive to send it. One proposal requires the originating computers to spend more time sending each e-mail by forcing them to perform more calculations as they contact servers to distribute those e-mails, thus reducing the number of messages a computer can send in a day and increasing the time and therefore financial cost. This delaying tactic could make spam much less attractive to senders who cannot expect enough of a response to make their mailing costs worthwhile (2004, p. 25). Such a system might well work as a deterrent for many spammers, including some con artists, but would no doubt require global cooperation that could be very tricky to design and enforce.

So for now, it still seems likely that for every antis spam measure someone develops, spammers will devise a countermeasure. Perhaps, then, preventing spam from reaching personal computers might better be treated as a secondary concern; the primary goal should in fact be the education of Netizens to recognize deceptive content, specious persuasive strategies, inaccurate and

unfair stereotypes of developing countries, and typical language features of a scam when they see them, ensuring that they will avoid becoming its next victim. And given the numbers of supposedly well-educated Americans who still fall prey to cons in other forms (phone and mail scams, for example), evidently still convinced that there *is* a way to beat the system and get rich without having to earn their success, it's neither surprising nor a black eye for the Internet that computer users are also susceptible. The bottom line, regardless of the medium, still has to be that oldest of financial clichés: if it sounds too good to be true, it most certainly is.

### References

- Baines, Harold. *The Nigerian Scam Masters: An Expose of a Modern International Gang*. Hauppauge, NY: Nova Science Pub., Inc., 1996.
- Baker, Stephen. "The Taming of the Internet." *Business Week* December 15, 2003: 78–80, 82.
- Bernstein, Judith H. "How to ... Avoid Net Scams and Dangers." *Newsday* [Nassau and Suffolk edition] January 19, 2009: B13. Retrieved May 28, 2009, from [http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T6660161865&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29\\_T6660161870&cisb=22\\_T6660161867&treeMax=true&treeWidth=0&csi=8320&docNo=5](http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T6660161865&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T6660161870&cisb=22_T6660161867&treeMax=true&treeWidth=0&csi=8320&docNo=5)
- Blommaert, Jan, and Tope Omoniyi. "Email Fraud: Language, Technology, and the Indexicals of Globalisation." *Social Semiotics* 16.4 (December 2006): 573–605.
- Brady, Diane. "My Shot at Nigerian Millions; I Answered an E-mail Promising a Fortune for Helping Desperate Foreigners Move Money Overseas. They Called Me—Then Got Cold Feet." *Business Week Online* April 24, 2003: 1–2. Retrieved June 7, 2004, from [http://web2.infotrac-custom.com/pdfserve/get\\_item/1/s1900eew2\\_1/SB638\\_01.pdf](http://web2.infotrac-custom.com/pdfserve/get_item/1/s1900eew2_1/SB638_01.pdf)
- Brown, Penelope, and Stephen C. Levinson. *Politeness: Some Universals in Language Usage*. Studies in Interactional Sociolinguistics 4. Cambridge: Cambridge University Press, 1987.
- Buechner, Maryanne Murray. "How to Kick Out the Trash." *Time* June 16, 2003: 52–3.
- Crampton, Thomas. "A Web Cadre Turns the Tables on African Scam Artists." *The New York Times* [Late edition] July 2, 2007: 7. Retrieved July 23, 2007, from [http://web.lexis-nexis.com/universe/document?\\_m=c23b26a4c758e1828371782def743f90&\\_docnum=2&wchp=dGLbVzb-zSkVA&\\_md5=6c28f7b0db60960dcecebcc86e5829d3](http://web.lexis-nexis.com/universe/document?_m=c23b26a4c758e1828371782def743f90&_docnum=2&wchp=dGLbVzb-zSkVA&_md5=6c28f7b0db60960dcecebcc86e5829d3)

- Cruikshank, Douglas. "I Crave Your Distinguished Indulgence (and All Your Cash)." *Salon* August 7, 2001: 1–4. Retrieved June 2, 2005, from <http://dir.salon.com/people/feature/2001/08/07/419scams/index.html>
- Denes, Shary. "Beware of E-mail Fraud." *Rural Telecommunications* July/August 2002: 8.
- Dudley, Gavin. "Nigerian Web Site Counters E-Mail Fraud." *Africa News Service* March 28, 2002: 1. Retrieved June 7, 2004, from [http://web2.infotrac-custom.com/pdfserve/get\\_item/1/S18fcf3w2\\_3/SB619\\_03.pdf](http://web2.infotrac-custom.com/pdfserve/get_item/1/S18fcf3w2_3/SB619_03.pdf)
- Dupin, Chris. "When 4-1-9 Equals 9-1-1." *The Journal of Commerce* 4.4 (January 27–February 2, 2003): 23–4.
- Ellis, Stephen. "UK Fraud Victims Lose Millions to Post Crooks." *The Daily Telegraph* [London] February 1, 2003: 6. Retrieved May 23, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=d43cacdd1d3e238badeef9ee48d910a&\\_docnum=32&wchp=dGLbVlb-zSkVA&\\_md5=bf8474ffe9e8923979e7bc11788a516b](http://web.lexis-nexis.com/universe/document?_m=d43cacdd1d3e238badeef9ee48d910a&_docnum=32&wchp=dGLbVlb-zSkVA&_md5=bf8474ffe9e8923979e7bc11788a516b)
- Emling, Shelly. "This Spoof Isn't Funny: Spam Used as Tool for Fraud." *Austin American-Statesman* July 10, 2003: C1. Retrieved July 29, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=be26a35c173645636ca324da4ef05ffe&\\_docnum=3&wchp=dGLbVtz-zSkVb&\\_md5=bdca44e9b977bde4574dd5b7024cd3](http://web.lexis-nexis.com/universe/document?_m=be26a35c173645636ca324da4ef05ffe&_docnum=3&wchp=dGLbVtz-zSkVb&_md5=bdca44e9b977bde4574dd5b7024cd3)
- Fowles, Jib. "Advertising's Fifteen Basic Appeals." *ETC: A Review of General Semantics* 39.3 (1982): 273–90.
- The Freeman Institute. "The Anatomy of a Nigerian 419 Scam." 2005: n.p. Retrieved May 23, 2005, from <http://www.freemaninstitute.com/419anatomy.htm>
- Gleick, James. "You Have Spam." *Australian Magazine* March 15, 2003: 16. Retrieved July 29, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=1fda30f1ee0519d2140be581502cfd67&\\_docnum=183&wchp=dGLbVzz-zSkVb&\\_md5=3db1c6bb3240a9d1ba7c2ed9b2aed84c](http://web.lexis-nexis.com/universe/document?_m=1fda30f1ee0519d2140be581502cfd67&_docnum=183&wchp=dGLbVzz-zSkVb&_md5=3db1c6bb3240a9d1ba7c2ed9b2aed84c)
- Goffman, Erving. "Designs and Fabrications," in *Frame Analysis: An Essay on the Organization of Experience*. Boston: Northeastern University Press, 1974, 83–123.
- Goldstein, Alan. "Growing Junk E-mail Traffic Has Become a 'Headache.'" *Hamilton Spectator* [Ontario, Canada] August 12, 2002: D10. Retrieved July 29, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=3550ff6bea5787e1788de3f3a33bdabf&\\_docnum=48&wchp=dGLbVtz-zSkVb&\\_md5=34b249bcee6db14d8b237c3448899aab](http://web.lexis-nexis.com/universe/document?_m=3550ff6bea5787e1788de3f3a33bdabf&_docnum=48&wchp=dGLbVtz-zSkVb&_md5=34b249bcee6db14d8b237c3448899aab)
- "Gone Phishing." *Time* May 3, 2004: 91.

- Holt, Stella, and Louise Berg. "How to Can Spam." *Legal Week Global* December 17, 2002: n.p. Retrieved July 29, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=edb9af46783a3bae682dcc03ba58491c&\\_docnum=18&wchp=dGLbVzz-zSkVA&\\_md5=cc424972b6b3225f4c3abbcc0e e11708](http://web.lexis-nexis.com/universe/document?_m=edb9af46783a3bae682dcc03ba58491c&_docnum=18&wchp=dGLbVzz-zSkVA&_md5=cc424972b6b3225f4c3abbcc0e e11708)
- Husted, Bill. "S. Africa Arrests 6 in Internet Fraud; Millions Lost in Scheme." *The Atlanta Journal-Constitution* May 24, 2002, home ed.: 3F. Retrieved May 20, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=1c6c4b65497f44c80c1bc873c12fb653&\\_docnum=59&wchp=dGLbVlb-zSkVA&\\_md5=d84dffe4495b1b75128f444a2304b40b](http://web.lexis-nexis.com/universe/document?_m=1c6c4b65497f44c80c1bc873c12fb653&_docnum=59&wchp=dGLbVlb-zSkVA&_md5=d84dffe4495b1b75128f444a2304b40b)
- Johnson, Steven. "Winning the War on Spam." *Discover* June 2004: 24–5.
- Koerner, Brendan I. "The Nigerian Nightmare: Who's Sending You All Those Scam E-mails?" *Slate* October 22, 2002: n.p. Retrieved May 23, 2005, from <http://slate.msn.com/id/2072851/>
- Lambeth, Jonathan. "Crooks Set Up Worldwide Web of Deceit: From Auction Fraud to the Nigerian Letter Scam, the Net Has Become a Thief's Paradise." *The Daily Telegraph* [London] April 2, 2002: 29. Retrieved May 20, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=1cbc4b65497f44c80c1bc873c12fb653&\\_docnum=66&wchp=dGLbVlb-zSkVA&\\_md5=2ace6e2dbd3bd08b62ec7ba79f7aca6e](http://web.lexis-nexis.com/universe/document?_m=1cbc4b65497f44c80c1bc873c12fb653&_docnum=66&wchp=dGLbVlb-zSkVA&_md5=2ace6e2dbd3bd08b62ec7ba79f7aca6e)
- Lipka, Mitch. "As Economy Worsens, Complaints About Internet Scams Increase." *The Boston Globe* April 5, 2009: 2. Retrieved May 28, 2009, from [http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T6660161865&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29\\_T6660161870&cisb=22\\_T6660161867&treeMax=true&treeWidth=0&csi=8110&docNo=6](http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T6660161865&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T6660161870&cisb=22_T6660161867&treeMax=true&treeWidth=0&csi=8110&docNo=6)
- McCormick, Gavin. "Nigerian E-Mail Fraud Flourishes." *Associated Press Online* April 11, 2002: n.p. Retrieved May 20, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=66e6b52ae37e4ea0a9dabd0d36caeff4&\\_docnum=1&wchp=dGLbVtz-zSkVb&\\_md5=d62c25c1fa4f800aad491377c1883c55](http://web.lexis-nexis.com/universe/document?_m=66e6b52ae37e4ea0a9dabd0d36caeff4&_docnum=1&wchp=dGLbVtz-zSkVb&_md5=d62c25c1fa4f800aad491377c1883c55)
- Mikkelson, Barbara. "Nigerian Scam." *Urban Legends Reference Pages: Crime (Nigerian Scam)* September 6, 2003: n.p. Retrieved May 23, 2005, from <http://www.snopes.com/crime/fraud/nigeria/asp>
- "Nigeria; Internet Fraud Value Rises 11 Percent in 2008 over 2007—Study." *Africa News* April 6, 2009: n.p. Retrieved May 28, 2009, from [http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T6660161865&format=GNBFI&sort=BOOLEAN&start](http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T6660161865&format=GNBFI&sort=BOOLEAN&start)

DocNo=1&resultsUrlKey=29\_T6660161870&cisb=22\_T6660161867&treeMax=true&treeWidth=0&csi=8320&docNo=5

“The ‘Nigerian’ Scam: Costly Compassion.” *FTC Consumer Alert* July 2003: n.p. Retrieved May 23, 2005, from <http://www.ftc.gov/bcp/conline/pubs/alerts/nigeralrt.pdf>

Norr, Henry. “Fast-Growing Fraud from Nigeria Uses Internet to Search for Suckers.” *The San Francisco Chronicle* September 8, 2002, final ed.: A6. Retrieved July 29, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=1fda30f1ee0519d21406e581502cfd67&\\_docnum=199&wchp=dGLbVzz-zSkVb&\\_md5=bba1459d45857adf677d4f536c5f7844](http://web.lexis-nexis.com/universe/document?_m=1fda30f1ee0519d21406e581502cfd67&_docnum=199&wchp=dGLbVzz-zSkVb&_md5=bba1459d45857adf677d4f536c5f7844)

Pye, David. “Putting the Lid on Spam; Weapons Like URL Blocking, Traffic Throttling and Signaturing Can Win Battles Against E-mail Spammers, But There’s No End to the War.” *The Globe and Mail* July 23, 2008: 20. Retrieved May 28, 2009, from [http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T6660161865&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29\\_T6660161870&cisb=22\\_T6660161867&treeMax=true&treeWidth=0&csi=303830&docNo=45](http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T6660161865&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T6660161870&cisb=22_T6660161867&treeMax=true&treeWidth=0&csi=303830&docNo=45)

Riga, Andy. “Taking on Nigerian E-mail Con Games Becomes a Crusade for ‘Scam Baiters’: Web Sites Describe Tricks Played on Fraud Artists Who Bilk People of Millions.” *The Gazette* [Montreal, Quebec] July 18, 2003: B1. Retrieved June 17, 2004, from [http://web.lexis-nexis.com/universe/document?\\_m=21182d18d09c1d2d42c7780f55fd9917&\\_docnum=21&wchp=dGLbVtz-zSkVA&\\_md5=797503202bac5ee275aed44617ed7d4](http://web.lexis-nexis.com/universe/document?_m=21182d18d09c1d2d42c7780f55fd9917&_docnum=21&wchp=dGLbVtz-zSkVA&_md5=797503202bac5ee275aed44617ed7d4)

Rosenberg, Eric. “Nigerian E-mail Scams Still Work; Obvious Frauds Continue to Find Victims.” *Pittsburgh Post-Gazette* [five star ed.] November 13, 2005: A-7. Retrieved July 23, 2007, from [http://web.lexis-nexis.com/universe/document?\\_m=c23b26a4c758e1828371782def743f90&\\_docnum=22&wchp=dGLbVzb-zSkVA&\\_md5=389cb0238f5e1be053365cd957b0670d](http://web.lexis-nexis.com/universe/document?_m=c23b26a4c758e1828371782def743f90&_docnum=22&wchp=dGLbVzb-zSkVA&_md5=389cb0238f5e1be053365cd957b0670d)

Schiesel, Seth. “Turning the Tables on E-Mail Swindlers.” *The New York Times* [final ed.] June 17, 2004: G1. Retrieved June 17, 2004, from [http://web.lexis-nexis.com/universe/document?\\_m=21182d18d09c1d2d42c7780f55fd9917&\\_docnum=1&wchp=dGLbVtz-zSkVA&\\_md5=82db8723e41950b538062ab0f853a356](http://web.lexis-nexis.com/universe/document?_m=21182d18d09c1d2d42c7780f55fd9917&_docnum=1&wchp=dGLbVtz-zSkVA&_md5=82db8723e41950b538062ab0f853a356)

Schronen, Johan. “Internet Cafes ‘Used for 419 Scam.’” *Africa News Service* February 17, 2004: n.p. Retrieved May 20, 2005, from [http://web5.infotrac.galegroup.com/itw/infomark/555/1/67410615w5/purl=rcl\\_ITOF\\_0\\_A113343993&dyn=4!xrn\\_10\\_0\\_A113343993?sw\\_acp=mtlib\\_a-bl](http://web5.infotrac.galegroup.com/itw/infomark/555/1/67410615w5/purl=rcl_ITOF_0_A113343993&dyn=4!xrn_10_0_A113343993?sw_acp=mtlib_a-bl)

- Shaw, Gillian. "Internet Scammers Beware: When Online 'Scam Baiters' Bite Back at the Hordes of Con Artists Filling Your Inbox, the Results Can Be Hilarious, Triumphant—and Even Dangerous." *The Ottawa Citizen* [final ed.] April 8, 2007: A8. July 23, 2007 [http://web.lexis-nexis.com/universe/document?\\_m=c23b26a4c758e1828371782def743f90&\\_docnum=5&wchp=dGLbVzb-zSkVA&\\_md5=6c4a2d91869a8b258a44103b657f0217](http://web.lexis-nexis.com/universe/document?_m=c23b26a4c758e1828371782def743f90&_docnum=5&wchp=dGLbVzb-zSkVA&_md5=6c4a2d91869a8b258a44103b657f0217)
- "SurfControl Reminds Companies To Be on Guard against New 'Brand Spoofing' Spams That Threaten E-Mail Users." *PR Newswire* July 8, 2003: n.p. Retrieved July 31, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=7d27e5fbed256363095b5bf6111e5aa&\\_docnum=0&wchp=dGLbVtz-zSkVb&\\_md5=f342f12f9ed0434715ba087363591f84](http://web.lexis-nexis.com/universe/document?_m=7d27e5fbed256363095b5bf6111e5aa&_docnum=0&wchp=dGLbVtz-zSkVb&_md5=f342f12f9ed0434715ba087363591f84)
- Tive, Charles. *419 Scam: Exploits of the Nigerian Con Man*. N.P.: Chicha Favours, 2002.
- United States Secret Service. "Public Awareness Advisory Regarding '4-1-9' or 'Advance Fee Fraud' Schemes." 2002: n.p. Retrieved May 23, 2005, from <http://www.secretservice.gov/alert419.shtml>
- Valetk, Harry A. "Spam Scammers Hit a New Low with Spoofed E-Mail." *New York Law Journal* 228 (16 September 2002): s6. Retrieved July 31, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=f2bbc9a811764af7af45465e421479be&\\_docnum=18&wchp=dGLbVtz-zSkVb&\\_md5=43036f42ee464841917b6199d41153fd](http://web.lexis-nexis.com/universe/document?_m=f2bbc9a811764af7af45465e421479be&_docnum=18&wchp=dGLbVtz-zSkVb&_md5=43036f42ee464841917b6199d41153fd)
- Woellert, Lorraine. "Out, Out, Damned Spam." *Business Week* August 11, 2003: 54–6.
- York, Thomas. "Sept. 11 Rouses Schemers Who Use E-Mail Red Cross Issued Warnings Authorities Warn People About Fraudulent Pitches for Charitable Donations." *Investor's Business Daily* October 31, 2001: 8. Retrieved July 29, 2003, from [http://web.lexis-nexis.com/universe/document?\\_m=883abbcbd4b797d7b106d344de30a395&\\_docnum=18&wchp=dGLbVtz-zSkVb&\\_md5=e56dfe73d678c7a3e89b47392da61729](http://web.lexis-nexis.com/universe/document?_m=883abbcbd4b797d7b106d344de30a395&_docnum=18&wchp=dGLbVtz-zSkVb&_md5=e56dfe73d678c7a3e89b47392da61729)

Copyright of ETC: A Review of General Semantics is the property of Institute of General Semantics, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.



Copyright of ETC: A Review of General Semantics is the property of Institute of General Semantics, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.