A Little Paranoia Can Go a Long Way

By Jill R. Sommer

Paranoia may not be a good thing most of the time, but when it comes to the Internet and scam artists whose objective is to steal our hard-earned money, a little paranoia is the best defense.

If you are active in any of ATA's language division listservs, you are probably aware of the various scams that have been targeting ATA members. For instance, many Spanish interpreters in the Ohio area recently received an offer from a gentleman named Daniel asking them to interpret at his wedding in Cincinnati (I'm sure members in other states received similar offers). In another instance, members of ATA's German Language Division (GLD) listserv received an e-mail from a Ghanan prince requesting an interpreter for his German-speaking wife and son during a 10-day shopping trip in New York City. This prince must have several wives who speak a wide variety of languages (I can't imagine how they communicate), because a member of my local ATA chapter, the Northeast Ohio Translators Association (NOTA), forwarded me the same request, only this time the prince needed a Japanese interpreter for his wife. I've heard this "prince" also hails from the Gold Coast and has a French-speaking wife.

These e-mails sparked a very interesting online discussion among ATA members, and proved once again that the division listservs are an important means of communication between fellow translators and interpreters to keep up-to-date with our industry. ATA Executive Director Walter Bacak reported these scams to the Internet Fraud Complaint Center and has published a list of Internet fraud tips from the National Consumers League's Internet Fraud Watch at www.atanet.org/internet_scams_2005.htm. (See page 34.)

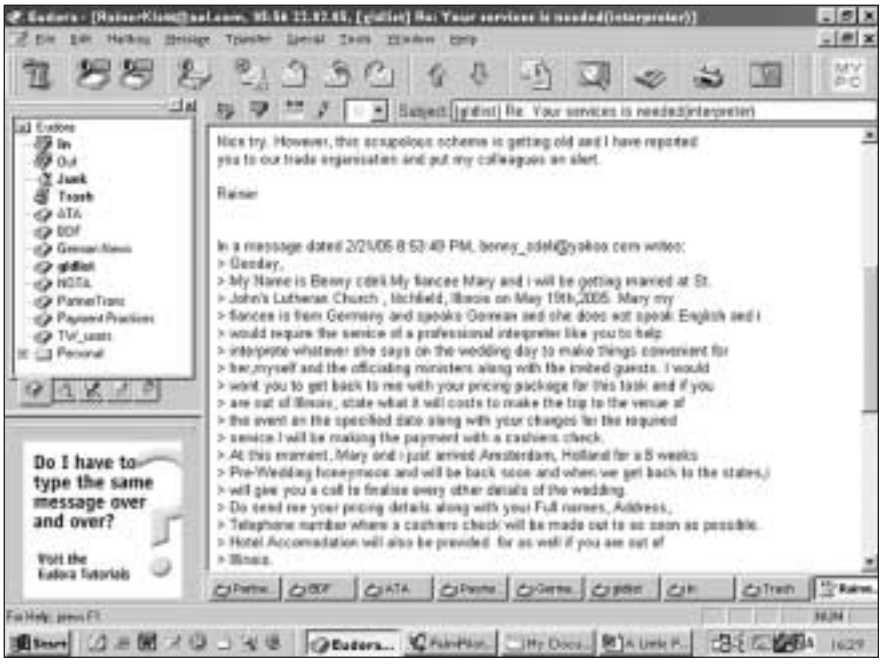
You may be asking yourself how the scams I just mentioned work, since the person doesn't ask for a social security number or any identifying information. The "customer" contracts for your services and asks you for an estimate. He then issues you a foreign draft or check for that amount, which might be fairly sizable, in advance to pay for your time.

> "…If a job offer seems too good to be true, it probably is…"

Once you deposit the check in the bank, the customer has a change of plans, for example, reducing the number of days needed for your services, or else "postponing" or even "canceling" the wedding. You are then asked to return most or all of the money "paid" to you. The scammer is counting on you sending him a real check that he can cash before your bank discovers that the check or draft you deposited is fake and that they can't collect on it. You will also receive a bill from FedEx a few days later for the shipping costs. This way the scammer manages to bilk you without ever having actually had access to your account—and you are left licking your wounds.

If a job offer seems too good to be true, it probably is. If a prince or rich businessman contacts you and suggests he pay you upfront before starting the job, please exercise ➡

Figure 1

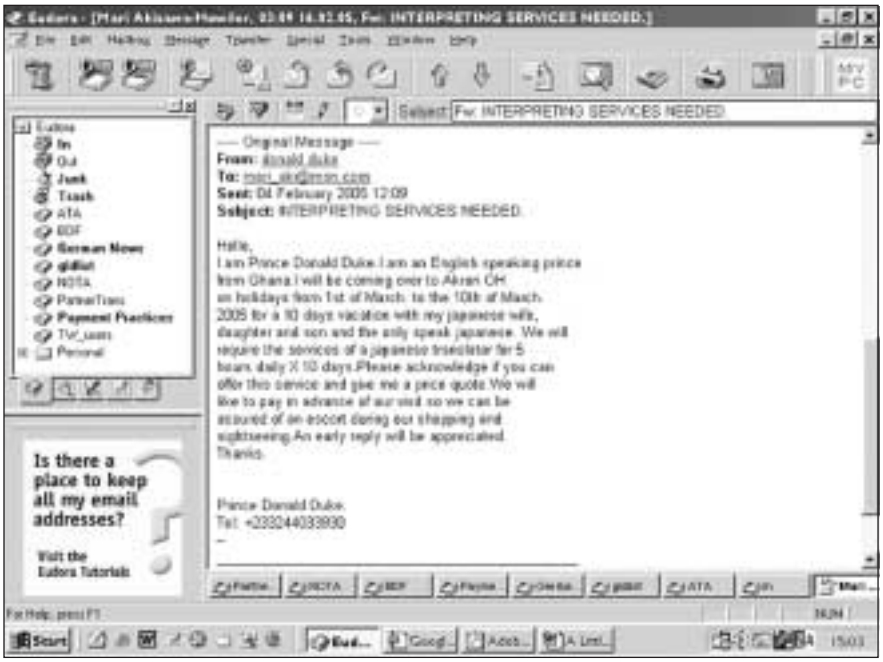


Some things in the above message should immediately raise red flags. First, most of our customers pay for our services after they are rendered. Second, the e-mail is not addressed to a specific individual, and the author's grammar and capitalization are abysmal. Third, how does the couple communicate if the fiancée does not speak English? And last but not least, who has time for a "pre-wedding honeymoon" right before the wedding? Most people are usually frantic with last-minute details at that point.

caution. Ask your colleagues if they have received similar requests. Forward the job request to ATA Headquarters or your local chapter to see if others have reported similar e-mails. If your local chapter or ATA language division has a listserv, this is the perfect venue to discuss the issue. Check out the local connections of the person (for example, see if there really is a wedding planned). Whatever you do, do not give anyone confidential information, such as your bank account or social security numbers, mother's maiden name, etc., without verifying that the person is who they say they are.

The idea of verifying bona fides applies to new agencies, banks, and anyone you do not know. If an agency calls and asks for my social security number—even if I worked with them recently and they need it for a 1099-MISC—I would much rather say I will call them back and look up the agency's telephone number in a reliable source, such as in ATA's online directories or on the agency's website. It is worth the price of a phone call to be reassured that my social security number is not going to end up in the wrong person's hands. Also, since I am extra cautious, I return the call from my landline phone, not my cordless or cell phone. Some cordless phones broadcast information as wireless signals that can be easily intercepted by an astute neighbor. I have a cordless stereo speaker in my office, and I can't tell you how many phone conversations have cut into my music when people nearby make a phone call from a cordless phone or call their cell phone voice mail to check their messages. Whenever that happens I simply change the frequency on the speaker, but someone sitting outside of your residence or business with a monitor or scanner may have more malicious intentions. Anyone with a baby monitor or cordless speaker can listen in on your "private" phone conversations—or, for that matter, any conversation you have in a room that has a baby monitor. For more information, see www.protectionconnect.com/0704wirelesssecurity.html.

Figure 2



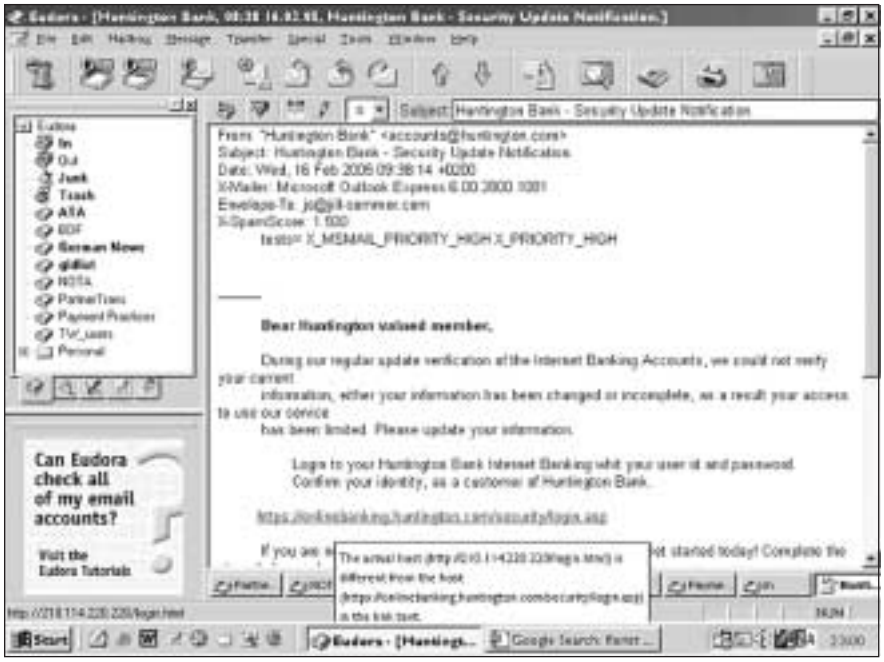
There are a couple things that should make you suspicious of this e-mail. First, the author capitalized all the letters in the subject line. Second, his grammar is questionable. His capitalization is quite good, except when it comes to the language his wife speaks (Japanese). He capitalized English correctly in "English speaking prince," but then consistently keeps Japanese in lower case letters. Last but not least, his return e-mail address is princedonaldduke@outgun.com. What prince would put his title in the e-mail? I would assume that he would want to maintain anonymity. Certainly Prince Charles doesn't send mail from "ThePrinceofWales@buckinghampalace.gov.uk." Also, I love Akron, but who wants to come to Akron in March for a 10-day vacation? Clevelanders and Akronites tend to flee to Cancun or the Bahamas in February and March!

If an individual or agency contacts you and you have never heard of them before, do some homework before accepting the job. Are they listed in the ATA directory? Do they have a website? You should also check the various online payment practice lists (see Ted Wozniak's article, "Ensuring Payment," April 2005 *ATA Chronicle)*. Ask for references from several current translators and do a Web search on the agency just to be safe. With careful research, you will hopefully never work for three weeks straight—forsaking all other clients—and end up empty-handed. I'm not saying agencies aren't to be trusted; my best clients are ATA corporate members. However, there are a few black sheep out there, so a little precaution is worth its weight in gold (or dollars—however you want to get paid!).

I don't know about you, but I think the Internet is the best thing since sliced bread. However, it has opened up new avenues for scams and con artists as well.

One popular e-mail scam is called

Figure 3



Here is a typical phishing e-mail. First , I am not a Huntington Bank customer. Second, when I hover the mouse over the link, you can see the actual host in the left-hand corner right above the Start button. My e-mail program (Eudora) also has a feature that opens up a warning message to inform me that the two addresses are different.

"phishing." Phishing is an attempt by criminals to trick unsuspecting consumers into disclosing personal and/or financial information. Although modern phishing scams tend to use e-mail, phishing can also be done via telephone, in-person, or via regular mail. For this article, let's concentrate on e-mail phishing. In this scenario, e-mails appear to come from companies with whom consumers may regularly conduct business (e.g., Huntington Bank, Earthlink, Paypal, eBay, or a credit card issuer). These e-mails frequently threaten termination of accounts unless consumers update billing information. Many e-mails also claim that the senders need to verify personal information they (allegedly) already have on file. They try to scare you so you don't think and merely act. The bottom line is that no legitimate company will contact you and ask for personal information in this manner. My bank is not a big-name bank and doesn't have my e-mail address, so the chances of them contacting me via e-mail is zero. As a result, it's easy to delete the e-mails from Citibank, Washington Mutual, Huntington Bank, and other financial institutions and go about my life. Even if you do use online banking and receive e-mail messages from them, banks and other serious businesses will never ask you for confidential information via an e-mail message.

However, I have been known to clear my clutter on eBay, so when eBay or Paypal contacts me to say my account has been suspended, I generally want to verify that everything is okay. If you ever receive an e-mail like this from anyone, catch yourself before you click that convenient link in the message to take you straight to the Web page. Chances are it's a fake that will lead you straight to a backdoor program or worm that will infect and wreak havoc on your computer—or much worse, it could be a con artist who wants to gain access to your personal information and possibly steal your identity. Don't take the bait! Assume any message could be malicious and use caution. It's easy for scam artists to create fake messages that contain return addresses, images, and URLs lifted from the actual company's website. Plus, scam artists are getting savvier and using reasonably well-written, grammatically correct, plausible text.

If the embedded link code (underlined and highlighted in blue by the e-mail program displaying it) uses numbers instead of the name of the site, chances are good that it's a fake. Every website resides at a specific Internet Protocol (IP) address, which is made up of numbers (such as 102.67.93.164). However, most web designers realize that people recall words more easily than numbers, so they don't publicize or advertise the numbers. Instead, they use words that are easy to remember and have some meaning to the company. For example, the IP address of NOTA's website is 65.211.123.67, but we direct everyone to "www.ohiotranslators.org." The address "www.ohiotranslators.org" is the real deal, but "www.ohiotranslators.scamcentral.org" could take you anywhere. Every domain name ends with a top-level domain like .com, .org, .net, or a country-specific top-level domain like .de (Germany), .uk (United Kingdom), .ca (Canada), or .ru (Russia). If the domain name is modified slightly or contains a word to the left of the title, the name (and the ➡

IP address) changes. Most phishers hope you won't notice or aren't aware of the difference. Another trick is to set up a website domain name whose spelling closely resembles the domain of a reliable, well-known company. For instance, it's easy to absentmindedly type "simantec.com" instead of www.symantec.com. This is not to imply that "simantec.com" is a scam, but it's certainly not the publisher of a well-respected virus protection program.

When in doubt, open a browser other than Internet Explorer (some of these e-mails have hidden code that can hijack your browser) and manually type in the company's website. Do not click on the link in the e-mail! If you are unsure of the website address, plug the company's name into Google (www.google.com) to find it. If it is a legitimate business, chances are good that it will be one of the first hits. Once you have entered the correct URL into your browser's address bar, skim through the site to find the page you need. For example, if you go to eBay (www.ebay.com), you will need to log in to reach your account information. If you find a page on the site with the same information noted in the e-mail, the e-mail was legitimate. If you don't find anything, you might want to contact the company through the contact information listed on the site. They may be unaware that a phisher is using the company's good name to do bad deeds. Either way, you haven't given away your valuable personal information. For more information on keeping e-mails private, go to email.about.com/od/staysecureand private/. For more information on phishing, visit antivirusabout.com/od/emailscams/ss/phishing.htm and www.identityprotection101.com/phishing. You may also want to learn how to identify online phishing fraud by taking the Phishing Test at www.mailfrontier.com/forms/msft_iq_test.html.

For those of you with websites, you need to be aware of the information you are putting out there, and make conscious decisions about what you are willing to publish about yourself. Some of our Kent State students have been cyberstalked in the past, so if a student expresses concern about publishing his or her address or other personal information, we encourage them not to do so. You may not want to put a photo of yourself on your website. My site does not list my home address. The only contact information on my site is my e-mail address and cell phone number. Back when the Internet and I were both younger, I was more concerned about the contact information that was out there, and wrote several sites asking them to remove my address. I'm not as concerned about cyberstalking these days, but I do regularly run Google searches on my name, social security number, and bank account numbers just to make sure the information currently on the Web is representative of what I want out there.

These examples are just the tip of the iceberg, but if you follow my suggestions and let yourself be paranoid once in a while, you will never regret it. A good rule of thumb is to avoid sending personal and/or financial information via e-mail whenever possible. When submitting financial information on a website, look for the "lock" icon in the bottom right of the browser's status bar to be sure your information is secure during transmission. Read a book or two on identity theft (I recommend *The Identity Theft Protection Guide* by Amanda Welsh), and remain vigilant at all times. A little paranoia can go a long way.

ata