Translation Scams: Tips for Avoiding Them and Protecting Your Identity

By Carola F. Berger

A lot of online scams

involving identity theft are hitting the industry these days. In many of these scams the victims' CVs/résumés are stolen by the scammers, who then use the information for their own criminal purposes. There are several basic categories of scams:

- The scammer impersonates the client/buyer.
- The scammer impersonates the language services provider.
- The scammer orders a translation from a translator but never pays.

People who actually check the names of the individuals with whom they are dealing can still be fooled into thinking that they are doing business with the real person.

This article will discuss a few of the common schemes targeting both buyers/end clients and translators/ language services providers, including how they work and how to avoid becoming a victim. While the examples discuss the scams as they apply to the translation profession, the underlying principles apply to other sectors and endeavors as well.

Why Would Anybody Impersonate a Client?

This is the age-old check-scamming trick, a variant of the Nigerian lottery scam. Here is how it works:

1) The client orders a translation, most of the time without haggling over price or without signing a contract, sending a purchase order, or any other written documentation. The entire transaction is done via e-mail, more often than not via a free e-mail account such as Google or Yahoo.

2) The translator delivers the translation and sends an invoice.

3) The client pays immediately by check, "accidentally" makes the check out for an amount larger than the invoiced amount.

4) The client tells the translator that the "accounting department" made a mistake and that the translator should just go ahead and cash the check and then wire back the difference or send a check for this amount. The client explains that this would be the best solution since it would be too complicated for the "accounting department" to remedy the error by any other means.

5) The translator goes ahead and cashes the check and sends back the amount that was overpaid.

6) A few weeks later, when the banking system finally finishes turning its wheels, it is discovered that the client's check is fake and the check bounces. The translator is charged with a bounce fee by the bank after already sending the client the amount that was "overpaid" on the fake check. Of course, in the meantime, every trace of the client's existence is erased, which means the translator has lost money for providing a service.

This and a few other variations of that scheme are actually quite common in the U.S. and all other places where payment by check is still prevalent.

> The main line of defense is to make it as hard as possible for somebody to impersonate you.

Why Would Anybody Impersonate a Translator?

Quite simply, people without the necessary skills need to impersonate reputable translators to obtain projects from unsuspecting clients.

1) The scammers impersonate reputable translators with stolen CVs, where they just edit a few contact details.

2) After checking out the impersonated translator's profile online, unsuspecting clients order translations from the fake translator under the assumption that they are getting a quality product.

3) The projects are then translated by the scammers via online open-source machine translation (a simple copy-and-paste operation) and sent back to the client without post-editing. More often than not, the client does not speak the target language and is therefore unable to judge the quality (or lack thereof) of the delivered product. (As an aside, machine translation by itself is not bad if it is implemented properly and post-edited, but these scammers skip this time-consuming step to make a quick buck.)

4) The client pays the scammers the amount invoiced. By the time the client notices that the translation is bogus, the scammers have long disappeared.

5) The client complains to the real translator who allegedly provided the fake translation. Both the end client and the real translator are the victims in this case. The end client has lost money and the real translator whose CV was stolen ends up with a damaged reputation.

There are many scenarios for these types of scams. An excellent resource with a comprehensive list of scam types is *The Scammers Directory* at www. translator-scammers.com. Along with the scammers' names, the site also lists the names of their victims. Please pay attention to the column headings in the table on the site so as not to confuse the scammers with the victims.

How Can Somebody Order a Translation and Get Away with Never Paying for the Service?

This is surprisingly easy if the buyer and the provider do not live in the same jurisdiction and there is no established dunning procedure between these jurisdictions. More often than not, any action taken to collect the outstanding amount would cost more than the amount owed.

ATA's website has a Business Practices resource section where you can obtain advice for dealing with bad payers (www.atanet.org/business_practices/ index.php). The site also contains tips on how to collect outstanding invoices, assuming that

you are dealing with a client who simply does not pay for some reason and not with an impostor as described above. Of course, the best way to prevent this situation is to vet your client thoroughly before you accept the assignment.

Verifying Identities and Payment Practices Online

The best protection against a scam is to verify that you are really dealing with who you think you are. Scammers generally fall into one of the following two categories:

1) **Scammers Who Do Not Try Too Hard:** They assume that they will eventually find a victim who is gullible enough. These types of scams are fairly easy to spot, as I will explain.

2) **Impostors Who Impersonate a Reputable Person:** People who actually check the names of the individuals with whom they are dealing can still be fooled into thinking that they are doing business with the real person, whereas all of their exchanges and transactions take place with the impostor. These types of scams are much harder to uncover.

Anybody with a computer and Internet access can open a translation agency today from anywhere in the world. While there are many very reputable agencies out there, there are also any number of fly-by-night "agencies" who are only looking to make a quick buck at the expense of translators and end clients. Therefore, if you are doing business with agencies, it is beneficial to become a member of various online forums that discuss payment practices or to subscribe to databases that list the payment practices of various agencies. Here is a list of forums and databases I consult regularly:

- **The Payment Practices Database**
  http://paymentpractices.net
  (A fee-based site.)

- **ProZ Blue Board**
  www.proz.com/blueboard
  (The overview is free, but the details are fee-based.)

- **Zahlungspraxis Yahoo Group**
  http://bit.ly/Zahlungspraxis
  (A free, very active site mostly for German-speaking countries/translators.)

- **World Payment Practices Free Yahoo Group**
  http://bit.ly/WPPF-group
  (A free site with a medium level of activity.)

- **Translation Agency Payment Yahoo Group**
  http://bit.ly/Agency-payment
  (A free site with a low level of activity.)

- **Translation Agencies Business Practices LinkedIn Group**
  http://bit.ly/Agency-business-practices
  (A free site with a medium level of activity.)

- **Unacceptable Translation Rates Naming and Shaming LinkedIn Group**
  http://bit.ly/Unacceptable-rates
  (A free site with a low level of activity.)

These are just a few among many, and your mileage may vary. I personally rely most on the Payment Practices database, but have also found the Zahlungspraxis Yahoo group quite useful.

> By setting up your own domain, it will become much harder for the scammers to impersonate you.

Impostors and Scammers: Typical Red Flags

So, are there any signals you should look for to help determine if you are dealing with a scammer? Indeed there are, but note that the presence of any one of the following warning signs alone does not mean that you are interacting with a dishonest person. All of these signs, combined with a few online checks, however, strongly point to a scam attempt. Your alarm bells should ring if you receive an inquiry that contains the following:

- The e-mail is sent from a free account, such as Gmail and Yahoo, etc. While this is not necessarily in itself an indication that the request is a scam/spam e-mail, the chances you are dealing with a scammer increase if the other factors discussed below apply. I have, in fact, several good direct clients who correspond via Gmail, but I am familiar with them from other sources and know they are legitimate. Most of my other clients, however, write via their corporate accounts.

- A proper salutation is missing and the e-mail is sent to my e-mail address via blind carbon copy. This type of e-mail points to the fact that this is a mass scam attempt.

- The request is written in really, really bad English, despite the fact that the sender claims to have a source text in English and identifies himself or herself with a name indicative of a native English speaker.

- The request does not contain any contact information aside from a generic e-mail address and possibly a telephone number in a foreign country. In general, this is a strong indicator that the e-mail is

a scam/phishing attempt. Everybody has an address and telephone number, and most people have a website these days. A name such as "Maria Brown," which is essentially un-Googleable because it is too generic, immediately raises red flags. If somebody really wants a translation, even if they have never bought a translation before, they give a name and address and possibly other contact information so that the provider can contact them with a quote. A name and address can also be used by the translator to search for the prospective buyer online and verify his or her existence, which I will explain below.

But what if you receive a serious inquiry from a person/company for whom you searched and found online with apparently proper contact information? You should still check out the potential client more thoroughly. For one, they could be impersonating somebody else, or they could be one of those black sheep on the translation market who never pay (and get away with it!).

Verifying IP Addresses and Internet Domains

Typically, impostors proceed as follows:

- They steal a reputable person's credentials. (Read on to learn how to safeguard yourself against this.)
- They modify the contact details to display their own contact information, possibly with a fake name.
- If they are smart, they use an e-mail address and possibly a domain name that very closely resembles the original address and domain.

I fell victim to this once when I was contacted by somebody purporting to be a project manager of a reputable agency. I checked out the agency and did my research, but what I did not notice was that the inquiry was sent from an e-mail address ending in ".net" instead of the agency's ".com." That is, the e-mail came from "projectmanager@translationagency.net" instead of "projectmanager@translationagency.com." Of course, when I checked out the agency, their website was at "www.translationagency.com." The scammers had simply temporarily bought the domain name "translationagency.net," since domain names are fairly cheap these days.

If somebody really wants a translation, even if they have never bought a translation before, they give a name and address and possibly other contact information so that the provider can contact them with a quote.

So, how can you check whether an e-mail/inquiry is legitimate if scammers buy domain names left and right? One way is to check the domain name via Whois (www.whois.net) and then check the IP-address from which the inquiry was sent. This is done as follows:

1) Visit http://centralops.net/co/DomainDossier.aspx.

2) Type the domain name into the search box and check the options "domain whois record" and "network whois record." The rest of the options may be a bit confusing.

3) The Domain Whois Record tells you who registered the domain and the name of the administrator, along with their address and telephone number. This is important if you receive an inquiry from somebody supposedly from the U.S. but who is in reality sitting someplace else.

4) The Network Whois Record tells you the IP address range of that domain. Every computer on the web has an IP address, uniquely identifying the computer's location and the computer itself (just like a phone number). The format for an IP address consists of four numbers separated by three dots (e.g., 123.4.56.789). This is important because you can check whether the e-mail that was sent really came from this domain, as I will explain in the next step. Checking the e-mail is optional because it does not always provide more information. The domain record should already give you lots of information.

5) If you do not want to check the e-mail IP address, skip the next two steps. Otherwise, go to your e-mail program or webmail and display the header information. (Headers contain tracking information for an individual e-mail detailing the path a message took as it crossed mail servers.) A good list compiled by Google explaining how to find the headers for various e-mail/webmail programs can be found at http://bit.ly/Google-message-headers. Once you have displayed the header, do not panic if what you see does not make sense. Instead, read on.

6) You can safely ignore everything in the header except the lines that start with "Received:". These lines represent a list of all the servers/computers through which the message traveled on its way to you. The top "Received" line is your own system. The last "Received:" line at the bottom is the computer from which the message was sent. You want to check this one

again at http://centralops.net/co/DomainDossier.aspx. (Yes, the search box also works with IP addresses). Of course, this may or may not correspond to the information you obtained from the domain name, because in this day and age some people reroute their e-mail through other interfaces.

By following these steps, you should now have a pretty good idea who contacted you and from where. Armed with this information you can do further research if the contact is a translation agency.

Protection Against Identity Theft

So, how can you protect your identity from being stolen in the first place? The main line of defense is to make it as hard as possible for somebody to impersonate you. Of course, it is never completely impossible to steal somebody's identity, but if you make it very hard, then the scammers will likely look for another victim and leave your reputation intact. Here are a few tips:

> Never post details that are too personal online.

1) Never post details that are too personal online, for example, your precise date and place of birth, your social security number, and other personally identifying details that are not needed to conduct business. Of course, in some countries you might be legally obligated to post this type of information. For example, in certain German-speaking countries such as Austria and Switzerland, local legislation requires you to post your tax number online in your "Impressum" (the term given to a legally mandated statement of the ownership and authorship of a document). I am talking about the equivalent of the Umsatzsteuer-ID, which is NOT your Steuernummer/tax ID/social security number. The former identifies your business; the latter identifies you as a person and can be used to impersonate you. Please check your local legislation regarding this matter and do not confuse the two ID numbers.

2) Get your own domain name and set up your e-mail to run through your domain instead of using a free provider such as Gmail, Yahoo, etc. By setting up your own domain, it will become much harder for the scammers to impersonate you. They will have to hack your account to do so. If you use a free e-mail account, a scammer can set up another account

Resources on Scams and Identity Theft

ATA Business Practices Resource Page
www.atanet.org/business_practices/index.php

ATA Members and Internet Scams
www.atanet.org/membership/internet_scams.php

Domain Dossier
http://centralops.net/co/DomainDossier.aspx

Federal Bureau of Investigation Scams and Security Information
www.fbi.gov/scams-safety/frauds-from-a-to-z

Fake Check Schemes
www.consumer.ftc.gov/articles/0159-fake-checks

Finding Message Headers
http://bit.ly/Google-message-headers

National Consumers League
http://fraud.org

National White Collar Crime Center
www.nw3c.org

The Scammers Directory
www.translator-scammers.com

Whois
www.whois.net

with a name very similar to yours and use that account to impersonate you. For example, if your e-mail account is "janedoe@freeemail.com," scammers could set up an account at "janedo@freeemail.com" and pretend to be you.

And no, you do not have to have your own website to own a domain name and run an e-mail account through that domain. However, having a website is always a good idea, even if it is just one page with your name and basic contact information. Most hosting providers, including mine, have simple tools that you can use to build your own rudimentary website. You do not have to be a graphic designer or a website wiz to set up a simple but good-looking page. And having a website does not break the bank these days either. Still, if you do not want a website, many providers offer e-mail-only options.

3) Do not send out your résumé or CV in plain text or Word format. Save it in PDF format instead and secure the document with a password.

Regarding Point 3, every word processing program with which I am familiar has the option to "Save as PDF." Plain text or a Word file is much easier to edit and tamper with than a PDF, especially if the PDF is protected by a password against editing. Obviously, you do not want to password-protect the file against viewing, so here is how to accomplish that with Adobe Acrobat, assuming that you have saved your document as a PDF file. Please note that the free Adobe Reader will not work for this. If you do not own Adobe Acrobat, there are freeware programs out there that allow you to password-protect PDF files. I personally am using Acrobat, so I cannot comment on other programs. Here are the steps for Acrobat:

1) Save your document as a PDF. This is accomplished easily in most word processors by simply choosing the option "Save as" and then choosing "Portable Document Format/PDF."

2) Open your PDF file in Adobe Acrobat and click on "File > Properties." Go to the "Security" tab and click on "Security Method > Password Security."

3) Set up password protection for editing. Obviously, you still want people to be able to view your document without requiring them to type in a password. You only want to protect the document against someone editing or copying and pasting the content. This is done with the following settings:

- Check "Encrypt All Document Contents."
- Uncheck "Require a Password to Open the Document."
- Check "Restrict Editing and Printing of the Document." Set the "Printing Allowed" and "Changes Allowed" options to "None."

4) Enter the "Change Permissions Password" and click "OK." A popup window will be displayed where you have to enter the same password again and click "OK." Click "OK" again when the warning is displayed. Close the dialog box by clicking "OK."

5) Save the document with the changed permissions. That's it!

Now your CV/résumé is password-protected against changes and copy-paste operations.

A Little Prevention

Taking steps to safeguard your identity and minimize the risk from scammers is not as difficult as it sounds, but it takes diligence. While no single tool or technique can guarantee total immunity from the constantly evolving methods employed by scammers, the information presented here should help you be more aware of how these individuals work and how they take advantage of the open community we have created on the web. ■

Don't Miss Out!

Many of ATA's announcements, including division newsletters, webinar schedules, and conference updates, are sent to members by e-mail. To be sure that these messages don't end up in your spam folder, take a minute now to add ata-hq@atanet.org to your "safe senders" list.