# TSD INFO BULLETIN

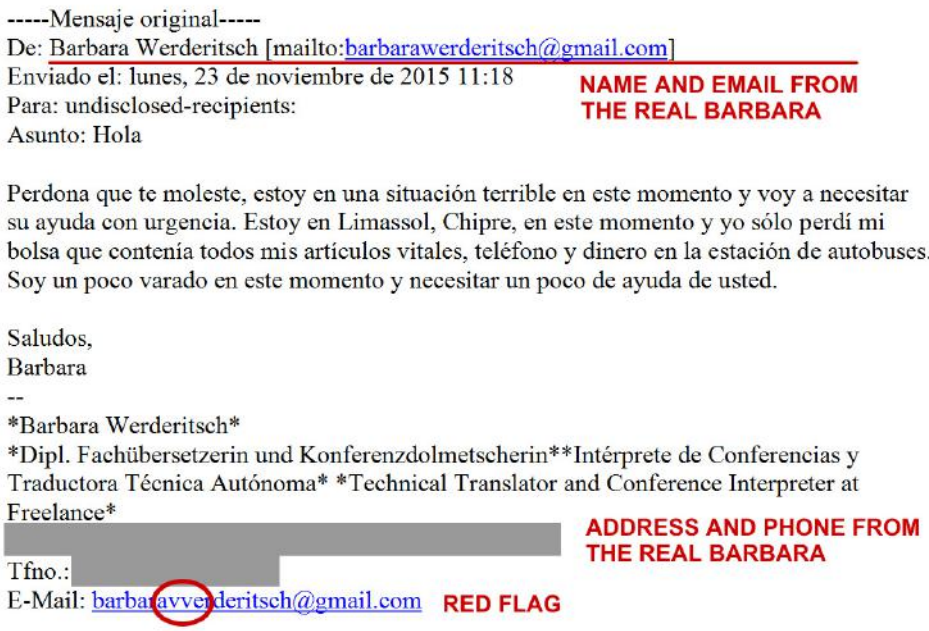
**by the TRANSLATOR SCAMMERS INTELLIGENCE GROUP**
**www.translator-scammers.com ● mail@translator-scammers.com ● @tsdirectory**
**Bulletin no.: TSD/03/2015**
**Date issued: 26 NOV 2015 ● Revision: 17 JUL 2016**
**Circulation: Worldwide**
**Special instructions: Sharing of this bulletin is appreciated**

## EMAIL HEADERS
## Their importance in the fight against scammers

Scamming, in all shapes and forms, is a game of deception. Scammers will play (or try to play) confidence tricks (synonyms include *confidence game, confidence scheme, scam* and *stratagem*) in an attempt to defraud a person or group after first gaining their **confidence**, used in the classical sense of **trust**.

Confidence tricks exploit typical human characteristics such as dishonesty, honesty, vanity, compassion, solidarity, misfortune, credulity, irresponsibility, naïveté and greed. Scammers will tug at your heartstrings with made-up stories about how they need (your) money — for emergencies, hospital bills, or to cover those unexpected costs... And, because we are human, we can fall prey of this psychological manipulation.

Consider the following email: Barbara is stranded in Cyprus, and she lost all her *"artículos vitales, teléfono y dinero"*. Again, because we are human, we can relate to the state of despair Barbara is going through… Typical impulse: let's help Barbara! — *What kind of stony-hearted person wouldn't do that for me, right?*



-----Mensaje original-----
De: Barbara Werderitsch [mailto:barbarawerderitsch@gmail.com]
Enviado el: lunes, 23 de noviembre de 2015 11:18
Para: undisclosed-recipients:
Asunto: Hola

NAME AND EMAIL FROM THE REAL BARBARA

Perdona que te moleste, estoy en una situación terrible en este momento y voy a necesitar su ayuda con urgencia. Estoy en Limassol, Chipre, en este momento y yo sólo perdí mi bolsa que contenía todos mis artículos vitales, teléfono y dinero en la estación de autobuses. Soy un poco varado en este momento y necesitar un poco de ayuda de usted.

Saludos,
Barbara
--
*Barbara Werderitsch*
*Dipl. Fachübersetzerin und Konferenzdolmetscherin**Intérprete de Conferencias y Traductora Técnica Autónoma* *Technical Translator and Conference Interpreter at Freelance*
[redacted]
ADDRESS AND PHONE FROM THE REAL BARBARA
Tfno.:
E-Mail: barbaravverderitsch@gmail.com RED FLAG

First rule about fighting scammers: **READ. ATTENTIVELY!** Scammers count on you not to. Let' read, then: you google Barbara's name and email address, and both point to a legitimate page on a translator's portal.

— *That's it! I'm going to help the poor damsel in distress* (misfortune, compassion, solidarity, credulity…).

But, before you send Barbara any money (what else can you do?), remember we said **READ. ATTENTIVELY.**

Let's read again, then: see that email address in the last line: barbara**vv**erderitsch@gmail.com? With **VV** instead of a **W** like in the email address in the first line? Congratulations! You've just busted another scammer: "Barbara" is not stranded in Cyprus without her *"artículos vitales"* after all.

**Always remember: ALL scams are about money! Your money! If your online sweetheart or Barbara in Cyprus asks for money, you can expect it's a scam.**

Sometimes, scammers are not so careless as to give you such prominent red flag in the open. That's why, at the least doubt about the genuineness of any message landed in your inbox, you should always analyze its header. The email header contains a detailed log of the network path taken by the message between the mail sender and the mail receiver(s) (i.e., the email servers).
**CLICK to know how to open the email headers on your webmail provider or email client/program.**

Let's open the header of "Barbara's" message:


There you have it (from top to bottom):

***Reply to:*** the address you'll respond to **(in this case, the SCAMMER'S ADDRESS)**.

***X-Original sender:*** the sender of "Barbara's" message (in this case, by means of SPOOFING). Email spoofing is the creation of email messages with a forged sender address. It is easy to do because the Internet email protocols do not have any mechanism for authentication. It can be accomplished from within a LAN, from an external environment using Trojan horses, or from anonymous or pseudonymous remailers.

Let's now see another interesting email received from a Ukrainian "translator":


For more information about "Luciano", visit **THIS LINK in our Directory**.

Let's read another email header. Remember: **ATTENTIVELY.**


We told you: email headers contain a lot of useful information. Read it. And use it.

And a final one, even scarier:

Received: from DBXPR06MB431.eurprd06.prod.outlook.com ([10.141.14.27]) by DBXPR06MB431.eurprd06.prod.outlook.com ([10.141.14.27]) with mapi id 15.01.0506.009; Tue, 24 May 2016 22:05:22 +0000
**From: karla adeson <karla0adeson0@hotmail.com>**
**Subject: Job App for Norwegian <> English professional freelancer translator**
Thread-Topic: Job App for Norwegian <> English professional freelancer translator
Thread-Index: AQHRoRtxhQJNLyHAzka7ctbEa22Dqp+e9P6HgAQsE8yAAiSVS4AAAPNLgAEMXlGABCRPP4AF+oZAgAI2dG2AAOMzIIAKSrzUgAGSPdf//zc8U4AHA3bsgADEJpWAAZ4ClQ==
Date: Tue, 24 May 2016 22:05:22 +0000
Message-ID: <DBXPR06MB431A15CBA12726525606517A84F0@DBXPR06MB431.eurprd06.prod.outlook.com>
References:DBXPR06MB43155A5E1602D91C7BAB9AAA8650@DBXPR06MB431.eurprd06.prod.outlook.com>,<DBXPR06MB43139346AB5FDCD7CB2C8FDA8650@DBXPR06MB431.eurprd06.prod.outlook.com>eurprd06.prod.outlook.com>,<AM3PR06MB42096D27492BC3C3F04A509A84E0@AM3PR06MB420.eurprd06.prod.outlook.com>
In-Reply-To: <AM3PR06MB42096D27492BC3C3F04A509A84E0@AM3PR06MB420.eurprd06.prod.outlook.com>
Accept-Language: en-CA, ar-SA, en-US
Content-Language: en-CA
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator: authentication-results: spf=softfail **(sender IP is 25.152.0.58)**
**smtp.mailfrom=hotmail.com; thetranscriptionagency.com; dkim=none (message not signed) header.d=none;thetranscriptionagency.com; dmarc=fail action=none header.from=hotmail.com;**
**received-spf: SoftFail (protection.outlook.com: domain of transitioning hotmail.com discourages use of 25.152.0.58 as permitted sender)**
x-tmn: [2Se+s1qQSNvyohPn/IoynZE+MDaJT4isseN4m4eJ4zg=]
x-eopattributedmessage: 1

**NOTES:**
**IN YELLOW**: data from false translator created by Gaza scammers.
**IN BLUE**: evidence of abusive use of the email server from **thetranscriptionagency.com.**
**sender IP is 25.152.0.58** (UK Ministry of Defence ???)
Info at: **https://db-ip.com/25.152.0.58**

**FINAL NOTE**
To avoid detection, CV scammers and translator impersonators frequently operate two (sometimes, even more) email addresses for each identity they hijack or create. If the scammer sends his email from a Gmail address, this is probably the only one created/used for his operation (but not always). Because their email is usually sent from a Gmail account (or other free email account), scammers close this account (once exposed, or just to bypass spam filters) and create a new Gmail, Hotmail, Yahoo, etc. address to keep sending their fake CVs.

For more information, read our guide **SCAMMERS, EMAILS AND EMAIL HEADERS**.