International Society for Labour and Social Security Law
Société internationale de droit du travail et de la sécurité sociale
Sociedad Internacional de Derecho del Trabajo y de la Seguridad Social

Dear colleagues,

In the past few days, many persons in our Society have received an e-mail, which appeared to be from our president, Janice Bellace. In the email, she asked for assistance. If the recipient of the email responded, the real sender then sent a longer message asking for money. At this point, many suspected correctly that the original email was not from Janice. This alerts us to a problem that is very common today – fraudulent emails. Please know:

1. The Executive officers of the ISLSSL would never ask you to wire money to them.

2. Only the ISLSSL treasurer would request a wire transfer of funds and the treasurer would direct you to wire your association's dues payment directly to the ISLSSL account with UBS bank in Geneva.

Some of you suspected that Janice's email account was "hacked." Janice had already contacted in the past her university's IT group and they report that her email account has not been hacked – but there has been fraud. They informed her that what had occurred was another phenomenon, called "spoofed" emails.

Here is an explanation from the website of a U.S. government agency:

If your business regularly makes wire transfer payments, it could be the next target of a fast-growing scam in which cybercriminals trick employees into transferring large sums of money to them by impersonating CEOs and other company executives in spoofed emails.

How does it work? The schemers first study their intended victims. Social media websites, a company's own website, and news reports can give employees' names, job titles, email addresses, and telephone numbers.

With a company's information, scammers can spoof, or fake, an email to an employee who they know can transfer money or pay invoices for the company, making the email look like it's coming from an executive officer, regular vendor or other trusted source. Once the money is wired, it can be nearly impossible to recover.

We suspect that a person went to our Society's website, www.islssl.org, and looked at the names and email addresses of the executive officers, and decided that Janice as president could direct other persons in the Society to send money. The person then looked at the names and email addresses for the presidents of our member national associations. (These are listed on our website http://www.islssl.org/home/executive/). We are informed that a person can send an email and make it appear that it has been sent from another email account, one which is a known and legitimate email account (technically how this is done is beyond our understanding). That is what happened here. (Some of you noticed that if clicked 'reply' another email address appeared in the "to" box such office43@gmail.com. That was the real sender, but unfortunately an email address that is unknown and untraceable.)

We are told that there is nothing we can do to stop this. Today anyone can go on the web and find names and email addresses. What we can do is be suspicious of unusual email messages, and be extremely suspicious of any email message that asks you to wire money. We urge you not to respond to such a message directly by clicking "reply" or by clicking on anything in the message and to delete these messages. If you receive a message and have questions about its validity, please do not hesitate to contact the Secretary General, Giuseppe Casale.

Many thanks,

Janice and Giuseppe

ciedad Internacional de Derecho del Trabajo y de la Seguridad Social

Queridos colegas,

En los últimos días, muchas personas en nuestra Sociedad han recibido un e-mail que parecía ser de nuestra presidenta, Janice Bellace. En el correo electrónico, ella pidió que se enviaran tarjetas de asistencia o de regalo. Si el destinatario del correo electrónico respondió, el verdadero remitente envió un mensaje más largo pidiendo dinero. En este punto, muchos sospecharon correctamente que el email original no era de Janice. Esto nos alerta sobre un problema que es muy común hoy en día: los correos electrónicos fraudulentos. Por favor, sepan:

1. Los oficiales ejecutivos de la SIDTSS nunca te pedirían que les enviaras dinero.

2. Sólo el tesorero de la SIDTSS solicitaría una transferencia de fondos y el tesorero le indicaría que transfiera el pago de las cuotas de su asociación directamente a la cuenta de la SIDTSS en el banco UBS en Ginebra.

Algunos de ustedes sospecharon que la cuenta de correo electrónico de Janice fue "hackeada". Janice ya había contactado en el pasado con el grupo de IT de su universidad y ellos informaron que su cuenta de correo electrónico no había sido hackeada - pero ha habido fraude. Le informaron que lo que había ocurrido era otro fenómeno, llamado correos "falsos".

Aquí hay una explicación del sitio web de una agencia del gobierno de los Estados Unidos:

Si su empresa realiza regularmente pagos por transferencia electrónica, podría ser el próximo objetivo de una estafa de rápido crecimiento en la que los ciberdelincuentes engañan a los empleados para que les transfieran grandes sumas de dinero haciéndose pasar por directores generales y otros ejecutivos de la empresa en correos electrónicos falsos.

¿Cómo funciona? Los estafadores primero estudian a sus víctimas. Los sitios web de medios sociales, el sitio web propio de una compañía y los informes de noticias pueden dar los nombres de los empleados, los títulos de los puestos, las direcciones de correo electrónico y los números de teléfono.

Con la información de una empresa, los estafadores pueden falsificar o alterar un correo electrónico a un empleado que saben que puede transferir dinero o pagar facturas para la empresa, haciendo que el correo electrónico parezca que proviene de un ejecutivo, un proveedor habitual u otra fuente de confianza. Una vez que el dinero es transferido, puede ser casi imposible recuperarlo.

Sospechamos que una persona fue al sitio web de nuestra Sociedad, www.islssl.org, y miró los nombres y direcciones de correo electrónico de los oficiales ejecutivos, y decidió que Janice como presidenta podría dirigir a otras personas de la Sociedad para enviar dinero. La persona entonces miró los nombres y direcciones de correo electrónico de los presidentes de nuestras asociaciones nacionales miembros. (Estos están listados en nuestro sitio web http://www.islssl.org/home/executive/). Se nos informa de que una persona puede enviar un correo electrónico y hacer que parezca que ha sido enviado desde otra cuenta de correo electrónico, una que es una cuenta de correo electrónico conocida y legítima (técnicamente cómo se hace esto está más allá de nuestro entendimiento). Eso es lo que ocurrió aquí. (Algunos de ustedes notaron que si hacían clic en "responder", otra dirección de correo electrónico aparecía en la casilla "para" como office43@gmail.com. Ese era el verdadero remitente, pero desafortunadamente una dirección de correo electrónico desconocida e irrastreable).

Se nos dice que no hay nada que podamos hacer para detener esto. Hoy en día cualquiera puede ir a la web y encontrar nombres y direcciones de correo electrónico. Lo que podemos hacer es sospechar de los mensajes de correo electrónico inusuales, y sospechar extremadamente de cualquier mensaje de correo electrónico que te pida que envíes dinero. Le instamos a que no responda a tal mensaje directamente haciendo clic en "responder" o haciendo clic en cualquier cosa del mensaje y a que elimine estos mensajes. Si recibe un mensaje y tiene preguntas sobre su validez, no dude en ponerse en contacto con el Secretario General, Giuseppe Casale.

Muchas gracias,

Janice y Giuseppe

ciedad Internacional de Derecho del Trabajo y de la Seguridad Social

Chers collègues,

Ces derniers jours, de nombreuses personnes de notre société ont reçu un courriel qui semble provenir de notre présidente, Janice Bellace. Dans ce courriel, elle a demandé que des cartes de présence ou des cartes-cadeaux soient envoyées. Si le destinataire du courriel a répondu, le véritable expéditeur a envoyé un message plus long pour demander de l'argent. À ce stade, beaucoup soupçonnent à juste titre que le courriel original n'était pas de Janice. Cela nous alerte à un problème très courant aujourd'hui : les courriels frauduleux. Sachez-le :

1. Les dirigeants de la SIDTSS ne vous demanderaient jamais de leur envoyer de l'argent.

2. seul le trésorier de la SIDTSS demandera un transfert de fonds et le trésorier vous donnera l'instruction de transférer le paiement des cotisations de votre association directement sur le compte de la SIDTSS auprès de la banque UBS à Genève.

Certains d'entre vous soupçonnaient que le compte de messagerie de Janice avait été "piraté". Janice avait déjà contacté dans le passé le groupe informatique de son université et ils ont signalé que son compte de messagerie n'avait pas été piraté - mais il y a eu fraude. Ils l'ont informée que ce qui s'était passé était un autre phénomène, appelé "spoof".

Voici une explication tirée du site web d'une agence gouvernementale américaine :

Si votre entreprise effectue régulièrement des virements électroniques, vous pourriez être la prochaine cible d'une escroquerie en plein essor dans laquelle les cybercriminels trompent les employés pour qu'ils transfèrent de grosses sommes d'argent en se faisant passer pour des PDG et d'autres cadres de l'entreprise dans de faux courriels.

Comment cela fonctionne-t-il ? Les escrocs étudient d'abord leurs victimes. Les sites de médias sociaux, le site web d'une entreprise et les bulletins d'information peuvent donner le nom des employés, leur fonction, leur adresse électronique et leur numéro de téléphone.

Grâce aux informations de l'entreprise, les escrocs peuvent falsifier ou modifier un courriel destiné à un employé qu'ils savent capable de transférer de l'argent ou de payer des factures pour l'entreprise, en faisant croire que le courriel provient d'un cadre, d'un vendeur habituel ou d'une autre source fiable. Une fois l'argent transféré, il peut être presque impossible de le récupérer.

Nous soupçonnons qu'une personne s'est rendue sur le site web de notre société, www.islssl.org, et a regardé les noms et les adresses électroniques des membres de la direction, et a décidé que Janice, en tant que présidente, pouvait demander à d'autres personnes de la société d'envoyer de l'argent. La personne a ensuite consulté les noms et adresses électroniques des présidents des associations nationales membres (dont la liste figure sur notre site web http://www.islssl.org/home/executive/). Nous sommes informés qu'une personne peut envoyer un courrier électronique et faire croire qu'il a été envoyé à partir d'un autre compte de courrier électronique, qui est un compte de courrier électronique connu et légitime (techniquement, la manière dont cela est fait dépasse notre compréhension). C'est ce qui s'est passé ici (certains d'entre vous ont remarqué que si vous cliquiez sur "répondre", une autre adresse électronique apparaîtrait dans la case "à" sous la forme office43@gmail.com. C'était le véritable expéditeur, mais malheureusement une adresse électronique inconnue et intraçable).

On nous dit qu'il n'y a rien que nous puissions faire pour arrêter cela. De nos jours, tout le monde peut aller sur le web et trouver des noms et des adresses électroniques. Ce que nous pouvons faire, c'est nous méfier des courriers électroniques inhabituels, et extrêmement suspects de tous les courriers électroniques qui vous demandent d'envoyer de l'argent. Nous vous demandons instamment de ne pas répondre directement à un tel message en cliquant sur "répondre" ou en cliquant sur un élément du message et de supprimer ces messages. Si vous recevez un message et avez des questions sur sa validité, n'hésitez pas à contacter le secrétaire général, Giuseppe Casale.

Merci beaucoup,

Janice et Giuseppe