www.ACTO-org.uk
info@acto-org.uk

# ACTO BOARD OF DIRECTORS

## GOVERNANCE & GOOD GUIDANCE NOTES FOR MEMBERS

Subject: **A warning about email scams to therapists**

Issue Date: **09 November 2018**

Last Update: **09 November 2018**

We would warmly welcome members sending contributions to this subject. These should be sent to info@ACTO-org.uk.

*The Board of Directors has put together these **Governance and Good Guidance Notes** in good faith for the benefit of ACTO members and the general public whom we serve. It has been prepared as honestly as it can been with the knowledge available. Nevertheless, the Board of Directors declines all responsibility for any inaccuracies and would encourage each reader to go and to their own research on this subject.*

---

A number of members have told us they have received scam emails. We are sharing this information with you to prevent you being scammed. Please remember this is criminal activity.

## Example Scam

*The email may appear to come from a potential client looking for sessions. The patient may say they are coming from abroad and require sessions when they are in the UK. They may give a list of days and ask for your bank details to pay in one go. Alternatively, they say they want to pay you by cheque or bankers draft in advance and ask for your address so they can post a cheque. These scams then involve the 'patient' cancelling the sessions and asking for the money to be refunded. As international cheques take so long to be cleared they rely upon the therapist not knowing this and sending them the 'refunded' money before the original cheque is cleared, effectively leaving the therapist out of pocket.*

There may be a lot more information included and variations on the above.

## What to do and what not to do as an online therapist

- *If you are not sure all you need to do is to send, as usual your information pack and application form. Do not engage in any other form of email exchange until and unless you are sure the client is bona fide.*
- We would advise you not to send your bank details (though of course these may be in your Information Pack somewhere but the robots are less likely to read this!).

- Never open an attachment unless you are sure of the source: do not open emails or especially attachments which you suspect as being scams.
- Do not respond or forward emails which you suspect as being scams.
- If in doubt, contact the person or organisation the email claims to have been sent by ... better safe than sorry. This is especially important if you think it might be from a colleague or client.
- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email. If you are unsure do not click at all but go to your web browser and search the website directly and contact that organisation directly.
- Do not make purchases or charity donations in response to spam emails. Always go to the web address by searching for it on your web browser.
- When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails. Similarly, delete all addresses of previous parties in the email string, before forwarding or replying.
- Most Microsoft and other email clients come with spam filtering as standard. Ensure yours is switched on. Ask you IT consultant to install a firewall and other protective software.
- Most spam and junk filters can be set to allow email to be received from trusted sources, and blocked from untrusted sources.
- *As online therapists we strongly urge you not to use hotmail, live, google or yahoo email addresses as these seem to be attacked most often.*
- Most internet security packages include spam blocking. Ensure that yours is up to date and has this feature switched on.

## What the scammers are trying to achieve and the risks to you as a therapist

This criminal activity is likely to be an attempt to get you to part with money and data, or destroy your data through malicious activity by getting through your virus checkers and firewalls. In more detail:

- Spam can contain viruses and spyware.
- It can be a vehicle for online fraud, such as phishing (an attempt at identity theft leading you to disclose private information such as passwords).
- Unwanted email can contain offensive images.
- Manual filtering and deleting is very time-consuming.
- It takes up space in your inbox and distracts you from genuine messages.

Whilst sending your bank details alone would not be enough (probably) for the scammers to gain access to your bank account, please remember that these emails are not from people directly but from criminals using artificial intelligence to send the emails robotically. They will be seeking to build your profile. One piece of information may not suffice but they may next send you a Facebook invitation and learn the name of your partner or pet (which probably account for a high proportions of chosen passwords).

## What is phishing?

Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations, or in our case “potential clients”. They usually try to trick you into going to the site, for

example to update your password to avoid your account being suspended. The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake designed to trick victims into entering personal information.

- The email itself can also look as if it comes from a genuine source. Fake emails sometimes display some of the following characteristics, but as fraudsters become smarter and use new technology, the emails may have none of these characteristics. They may even contain your name and address.
- The sender's email address may be different from the trusted organisation's website address.
- The email may be sent from a completely different address or a free webmail address.
- The email may not use your proper name, but a non-specific greeting such as "Dear customer."
- They convey a sense of urgency; for example, the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website. Be most very careful to check before accessing such links. Our advice is never to hit these links but to go to that organisation's website directly.
- A request for personal information such as username, password or your bank details.
- You were not expecting to get an email from the organisation that appears to have sent it.
- The entire text of the email may be contained within an image rather than the usual text format. The image may contain an embedded link to a bogus site
- The email may include an attachment that the scammers tell you is information about themselves and their problem and that it can be opened with a password which they provide! Do not open it!

## How to spot a scam or spam email

- You don't know the sender.
- Contains misspellings (for example 'p0rn' with a zero) designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.
- Contains an urgent offer end date (for example "Buy now and get 50% off").
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.
- Contains attachments, which could include .exe files including the request to open an attachment which is password protecting and they include the password.
- Attempts to use your website's good reputation to send spam.

**Keep safe and secure!**

---

We would warmly welcome members sending contributions to this subject. These should be sent to info@ACTO-org.uk.