Charity Fraud Awareness Week

Options
Support | Empower | Enable
Living life to the full!

22nd – 26th October 2018

IN THIS ISSUE

IT'S FRAUD AWARENESS WEEK!

Like any other charity, Options is not immune to the threat of criminal abuse from fraudsters. Fraud poses a serious risk to valuable funds and sensitive data, it can damage the good reputation that has been built up, affecting public trust and confidence in an organisation.

MISUSE OF CHARITY MONEY

It is never pleasant to think that staff working at Options may be capable of fraud, but the reality is that more and more organisations are suffering from this. Misuse of charity money can come in numerous forms, from pocketing cash, misusing charity credit cards and increasingly cyber-crime.

A common example which we need to be wary of is false expenses.

False expenses are a method of internal fraud by claiming over-inflated, non-existent or inappropriate expenses or overtime. We need to ensure all expense claims are as described on the claim form, are accompanied by a receipt, submitted on time and are suitably authorised.

The risks to Options from cyber-fraud are increasing all the time.

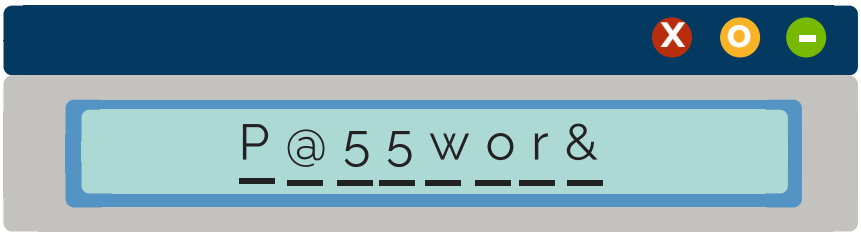
Cybercrimes can be quite complex and difficult to detect, often involving data breaches or identity fraud. As an organisation it's important to consider how best to protect Options' valuable data from harm online.

SOME OF THE COMMON CYBERCRIMES TO LOOK OUT FOR ARE:

- **MALWARE** – This is malicious software, including viruses, which can be reduced by using anti-virus software and a robust firewall.
- **PHISHING** – This is when bogus emails claim to be from legitimate sources, often containing an attachment or directing you to a scam website. If in doubt, speak to the individual sender and look for obvious signs of spam emails such as bad spelling or grammar.

MEASURES OPTIONS CAN TAKE AS AN ORGANISATION INCLUDE:

1. **Choosing strong passwords:**
Passwords are a free, easy and effective way to protect data if they're robust. It's best to use alpha-numeric characters and random symbols (such as @, & and *)



2. **Making sure electronics are secure:**
Always keep your smartphones and laptops safe when outside the office. Switch on device location apps so they can be found or data erased in the event of loss. Avoid public wi-fi spots as these maybe less secure. Ensure passwords are in operation on all devices.

3. **Getting confirmation:**
Make sure any changes to internal data is received in writing and confirmation is sought from the staff member or person we support of the intended change before being implemented.

OUR NEXT STEPS...

The crucial lesson for Options isn't about introducing lengthy counter-fraud policies. It's about changing people's behaviours and encouraging staff, people we support and friends of Options to be vigilant.

This must be demonstrated by everyone in our organisation to be truly effective. A dangerous combination of a lack of accountability and controls not being consistently applied can make any charity – big or small – vulnerable and create opportunities for fraudsters that will have devastating effects.

Let's not be one of the statistics!

To find out more about Fraud Awareness Week, visit:
www.gov.uk/government/news/charity-fraud-awareness-week-22-26-october-2018

Peter Jones
Finance Manager
0151 236 0855
pjones@optionsforsupportedliving.org

Did you know?

Reality star Kim Kardashian was recently named the riskiest person to look up online in the UK because of the number of search results containing links to malicious sites?

Actress Emma Roberts also featured in the top ten list that the cybersecurity firm McAfee noted... Good job it wasn't our very own Emma Roberts from our Personnel Team!