Scottish Social Services Council

Cyber resilience

Real life cases

£200k email scam hits Glasgow business

An employee at a Glasgow media firm transferred £200k to a cybercriminal who impersonated their boss via email in what is known as a business email compromise. They ignored bank warning messages about exactly such a scam as they proceeded through the online transfer process.

The employee was dismissed and later sued. Management were unaware the employee even had access to the firm's online banking.

Source: **BBC News** 7 February 2019

Social work case files found on Google

An Aberdeen City Council social worker downloaded case files from her work email to her personal computer. These were immediately uploaded to the internet and made public by software running on the computer.

The files were discovered by another worker during a Google search.

Aberdeen City Council was fined £100k by the Information Commissioner.

Source: **itpro.co.uk** 30 August 2013

Small Blairgowrie travel firm hacked

Cyber criminals were able to impersonate a small travel firm after gaining access to and redirecting visits to the 'contact us' page on their website.

They sold bogus holiday packages to customers. Staff at the real company were flooded with telephone calls from people who believed they had booked long-haul flights with them.

This was a sophisticated scam that involved setting up call centres, fake online identities to impersonate the Blairgowrie firm and days, if not weeks, of target research.

Source: **The Courier** 14 December 2018

Care home fined for stolen laptop

A domestic burglary resulted in the theft of a laptop containing sensitive information about care home staff and residents.

The laptop's hard disk was not encrypted. Management believed having a password on the user account was enough to prevent unauthorised access to the data. The Information Commissioner fined the care home £15k and they were heavily criticised for inadequate IT security.

Source: **carehome.co.uk** 26 August 2016

GPs and hospitals hit by ransomware

A devasting infection of WannaCry ransomware disrupted NHS services across Scotland and England. Made possible because these services ran out-of-date software with known security vulnerabilities.

Although not deliberately targeted at the NHS, it shows how indiscriminate cyber-attacks can be and how the impact on care services can be devastating.

Source: **BBC News** 13 May 2017

Social worker emails case files to personal Yahoo account

A locum social worker in England forwarded documents to their personal email account so that they could continue working on them during disruption caused by a new IT system.

This was later discovered by the local authority when the worker's contract came to an end and their work email account was examined for work that needed to be completed.

The worker was given a three-year caution by the Health and Care Professions Council (HCPC).

Source: **Community Care** 11 April 2019

10,000 care home and NHS staff passwords sold online

A data breach at an online training company revealed the email addresses and passwords of 10,000 NHS and care home staff.

Password reuse led to fears other online accounts belonging to those affected may have been accessed.

The stolen details sold on the Dark Web for 10 time the price credit card details would normally sell for. An indication of how much this information is worth to cyber criminals.

Source: **The Inquirer** 13 August 2018

SSSC

?

Scottish Social Services Council

THANK YOU