Cybersecurity for Charities

# Cybersecurity Briefing



## Introduction

Identity theft is a crime. It's a term that is used when someone unlawfully collects private information about somebody else, for instance, their national insurance number, address, date of birth, credit card numbers, passwords and PIN numbers, details of a loan application and so on. When someone has sufficient private information about you, they can masquerade as you.

## Learning Points

### Bit by Bit

Criminals are getting very good at collecting your personal information. One technique is to rummage through rubbish to find documents containing information about you that could be useful, a technique known as 'dumpster diving'. Although rather laborious this technique can prove most fruitful. Of course, hacking computers and specifically searching for useful information can be done from the comfort of their armchair, but most common are social engineering techniques that entice you to willingly give up what you know and they shouldn't.

Criminals are known to keep a log of the details they have about a person, and over time, often through social engineering, find data about you that is missing. So, someone calls you and asks for the second and last character of your password, then after you have provided it they make out that they didn't hear or understand or the line dropped, so they ask for the first and third instead. Bingo!, a few more blanks completed. Oh, and whilst I am on the line can you confirm your mother's maiden name, Hart isn't it? If it is, then another piece of data is qualified, if it isn't you may be helpful and tell them what it really is. Once there is sufficient info in their records they can now exploit your identity for whatever purpose. Let the masquerading begin.

### Make it difficult

A simple and effective strategy to prevent disposed documents from getting into the hands of the wrong'uns is to shred anything that contains personal information. This applies at home as much as it does in your workplace, and confidential documents you are working on should always be locked away when not in your hands. Remember also that eMails are about as public as a postcard. So don't attach private documents to an eMail unless you have put something in place to prevent it from being read. It could easily fall into the hands of someone else just by addressing the eMail incorrectly!

From a work perspective, your organisation's data is also precious. By not taking good care of it you increase the risk of financial, legal and reputational damage. For a charitable organisation any incident that exposes these vulnerabilities to the public can have devastating consequences. Take note of what you should be doing to protect it.

### Tips

- Shred personal, private and confidential documents, whether work or home based, before disposing of them
- Don't leave personal, private and confidential documents lying around for all to see. Keep them in a locked cabinet
- Never disclose personal or confidential information over the phone unless you have verified the caller. Better still, call them back on an official number, not the one they have provided to you
- Carefully check your bank and credit card statements for transactions that you do not recognise
- Adopt secure printing wherever possible, or use secure processes when printing personal or confidential information to a shared printer
- Password protect all your devices, especially mobile, and change them regularly, as they are often where you store your personal information

### Next Steps

- Do an audit of where your personal and/or confidential information is stored. Put in place practices to protect this privileged data.