iProfile

Secure your CV

Overview

ID fraud is one of the most serious issues facing people today. 100,000 people in the UK are victims of ID theft each year and one of the ways criminals can acquire people's personal details is by stealing information held on their CV. iProfile carried out a controlled experiment to assess the extent to which people are exposing themselves to identity theft. This report contains an overview of the experiment, the results and outlines the steps that job seekers can take to protect their identity when applying for jobs.

About the Experiment

The controlled experiment was conducted during, but independently from, National Identity Fraud Prevention Week (6-12 October 2008) – a time of supposed heightened awareness. The experiment was run by iProfile and was supported by the Metropolitan Police and the Information Assurance Advisory Council (IAAC).

A fake job advert for a company called Denis Atlas (an anagram of 'steal an id') was placed in a national newspaper to understand how many people would send their CVs without first checking out the company. If anyone searched for the company, they would have been taken to a website that was created as part of the experiment explaining that that the company did not exist. The site also contained further information about the experiment, the risks associated with CV ID fraud and advice to consumers on how to avoid identity theft.

All CVs received as part of the experiment were destroyed, without being stored or shared, applicants were also informed that they were part of a controlled experiment, and that they would not be identified in any way.

A reformed identity theft criminal, Bob Turney, was also enlisted to analyse the CVs to understand whether they contained enough information for an identity theft to occur.

The Results

107 people responded to the fictional job advert by sending their CV. 68% of people did not background check the company mentioned in the advert.

"Typically, criminals need just three out of fifteen key pieces of information to commit identity fraud.

The average CV received as part of the research project contained eight pieces of information."

Rather than using a traditional CV, think about using an iProfile - a free online CV service that helps safeguard your personal details.

Typically, criminals need just three out of fifteen key pieces of information to commit identity fraud. The average CV received as part of the research project contained eight pieces of information.

The research also revealed:

- 61 CVs (57%) included a date of birth, despite this no longer being a requirement due to age discrimination laws
- 98 (91.5%) included a full address
- 20 (19%) put others at risk by providing full details of references
- One CV even included the applicant's passport number and national insurance details

Protecting yourself from CV ID Fraud

- Be wary if the email address does not contain the name of the company but just the name of a service provider.
- Take extra care when accessing personal information when using public computers, such as those in internet cafes, or when using a laptop in a WiFi hotspot.
- Shred or destroy old copies of your CV.
- Rather than using a traditional CV, think about using an iProfile - a free online CV service that helps safeguard your personal details.
- Use a phone masking service to protect your personal number. With an iProfile you get phone masking, and it costs you nothing.

Think about who you share your career information with, make sure they are a real business and when posting your information to the web or on a job board database, remember to use an Internet Safe CV:

- Do not include your date of birth
- Do not include your marital status
- Do not include your place of birth
- Only give your first and last name
- Use a telephone masking service so you don't publish your private phone numbers

Think about the information a potential employer needs to find your details, you can share your full CV at a later stage when you are comfortable with the identity of the company or person you are sharing the information with.

How iProfile Safeguards Your Information

With an iProfile, you get security advantages over CV posting websites and the peace of mind that goes with knowing your identity is safe. Here are some of the safeguards built into the iProfile system:

- You decide who you share your details with, you are in control.
- Your iProfile is only accessible to the iProfile compatible agencies you have previously sent your CV to. You can select and can check which agencies have access and make changes to those permissions at any time.
- Everyone who views your iProfile has to log in first. Our software tracks those log-ins, so you know exactly who has viewed your CV and when.
- CVs sent via word document can't be controlled because they are distributed so easily. But with an iProfile, you simply send recruiters a link to your iProfile. You can remove access to that link at any time.
- You have a central place to keep track of the jobs you have applied for and the people or companies that you have sent your CV to.
- We don't sell our users' information. We don't even look at it. Only you and the recruiters you designate will ever see your iProfile posting.
- You can use our phone masking service to disguise your personal phone numbers. All calls received on this masked number are automatically forwarded to you and you can deactivate it at any time.

For all these reasons, an iProfile is much safer than hosting your CV on your own website, posting it to a social site, and is also much safer than sending a 'traditional CV'.

An iProfile is quick, easy and free to build, simply sign up at **http://www.iprofile.org**

Everyone who views your iProfile has to log in first. Our software tracks those log-ins, so you know exactly who has viewed your CV and when.

Metropolitan Police
Detective Superintendent Russell Day
from the Economic and Specialist Crime Command:

"The Metropolitan police are happy to support any campaign which aims to raise awareness of the growing threat of online Identity fraud. We advise all users to never post personal details on the internet which could collectively be used to clone your identity. This new campaign is an excellent method which could help prevent Identity fraud and most importantly, to protect you and your CV."

METROPOLITAN POLICE

Rick Bacon,
CEO of iProfile:

"People need to be aware of the dangers of posting personal information online. As people wise up to shredding their utility bills and bank statements, they should consider other material that fraudsters can use to steal their personal identity. The public need to treat any documents that contain personal information with care - including their CV. We hope this research highlights the dangers and gets people thinking about using the secure tools that are available on the internet to protect themselves."

iProfile

Neil Fisher,
Vice Chair, IAAC:

"Identity fraud is currently, and will remain, a hugely serious issue and any campaign that raises awareness of the dangers should be commended. Many people feel comfortable about sending their CVs 'blind' without thinking about the consequences if their information fell into the wrong hands. This campaign will help people better understand the risks they face if they do not take proper control over their personal information."

IAAC