

**Footprinting Report**

By

Robert Gabriel and Adrian Chambers

Note as its difficult to show the information, we provided links too :)

Footprinting is a technique used to gather information on a computer system. The accumulated data can then be used to exploit the system. Information can be gathered in non-intrusive ways such as through a company’s own website. Employees of a company may be targeted to see if they may have unwittingly supplied information that may be used against the company that they work for. This report will focus on a chosen target of a company and will describe ways the information provided by the target can be used negatively against the company.

The company we have chosen to footprint is Microsoft Ireland. We have chosen to gather information on one particular target, Stephen Howell, an Academic Engagement Manager for the company. As expected of an employee in the IT sector, he has a high online presence. Below is an outline of the information that we were able to gather:

* Multiple email addresses that are or have been used by the chosen target.
* Social sites that the chosen target is active on e.g. Twitter, Google+, Tumblr & Linkedin.
* Websites owned by the chosen target (saorog.com).
* The number of children he has and their names.
* Wife’s details (including place of work, interests & family details).
* Home and work address.
* Work History.
* Online aliases (saorog and v-sthowe)
* Server log location.

One may ask “what can be done with this information about Stephen Howell?” All the pieces we found on the web through the social media networks gave us an idea of who Stephen was and how well known he was online. As mentioned earlier he works as the education lead for Microsoft but is also the creator of the super popular Kinect 2 Scratch. Through the use of looking up his name on Facebook, LinkedIn, Twitter, Dravinart, News reports, planning permission information and more shockingly using “Geo tagging” with photographs, we were able to find his location as a result. From the information gathered, it seems that there are many ways that it can be used to exploit the target and garner further knowledge of the company that he works for. Below we will analyse some of the methods that may be used.

**Method 1:** Since we were able to gain his address online this could lead to an in-person attack. The attacker could possibly observe the family patterns and dumpster dive to gather more information. This technique could be used in a few locations such as Microsoft headquarters, the chosen target’s home or even the workplace of his wife.

**Method 2:** The chosen target provides a lot of information on his social sites that could inform an attacker of his schedule which could then allow an attacker to monitor his home and if possible break in and steal any information that may aid the attacker in finding out more information about Microsoft. This could include stealing his laptop – photos easily available online show his laptop so this can aid an attacker to help them directly target the specific item.This could possibly give us access to the source code to Kinect 2 Scratch and any other projects he may be working on as well as to servers for thousands of users as well as the Microsoft servers.

**Method 3:** Other social engineering techniques can also be used since the chosen target’s childrens’ names are known. It is possible an attacker could ring a receptionist of Microsoft while the chosen target is working and could claim that one of his kids are sick and need to be collected from school. This could provide an attacker with an opportunity to try and access the chosen target’s office to find more information or inform the attacker that the chosen target may not be working from the office on that day.

**Method 4:** Providing so much family information can easily help an attacker construct an email type attack, by using the chosen target’s childrens’ name in an email or even his wife’s workplace title. If the email is opened or if any executable file is downloaded this could possibly compromise the system.

**Method 5:** The chosen target predominantly uses the online alias ‘saorog’ and has used ‘v-sthowe’ which an attacker may flag to use as a username or password to access the chosen target’s files. His childrens’ names could also be candidates for this purpose.

**Method 6:** Do the ‘reset password’ option for his email using the personal information we know, to try gain access through the ‘reset password’ security question.

From what we have gathered, the chosen target’s digital footprint does not tend to leave any trace of comments or information that may directly compromise Microsoft, as expected an individual working in the IT sector are generally aware of the threats of their digital footprint. They would not provide too much information or links to inappropriate sites or photos. Although in some cases, it is possible that the information may have been supplied before they got involved in the IT industry, in this case once the individual comes aware of their digital footprint and the negative impact it can have upon them they can follow guidelines, such as removing inappropriate content, making sensible decisions on who can access the information, being wary of comments made by others, setting social network sites profiles to “private” and always consider the consequences of a post. This can be applied by anyone who becomes cautious of their digital footprint and though it does not provide complete online invisibility, it’s certainly a starting point.

# Conclusion

To conclude, footprinting is a well known method used to gather information on a computer system. Our chosen target for this assignment is an established IT user with a predominant online presence and he is clearly extremely careful in relation to the information that he provides, ensuring it does not implicate Microsoft. Even though the chosen target was quite cautious about providing in depth details online, we were still able to accumulate enough information on him and his family for a potential attacker to build a profile and use a variety of techniques to attempt to attack the Microsoft network. While port scanning and other techniques could be used to gather more information, they are beyond the scope of this assignment.

Privacy settings have become a large part of Social Networks in recent times and many people are following the steps to make their profile exclusive to their own friends and colleagues. We feel that if we were to carry out this assignment eight to ten years ago, we would have found a lot more information on an individual but with the high rise of potential employers observing people’s digital footprint before they even hire a new employee as well as current employees losing their jobs as a result of their online footprint, individuals are showing extra vigilance upon sharing information online at all times. We felt quite uncomfortable finding all this information on a stranger yet it took us only four or five hours to find a substantial amount of data on our target. Society as a whole needs to be vigilant when sharing information online. It’s truly frightening how individuals can find such large quantities of information in such a small period of time. Remember to be careful when sharing information on the internet!



References

Name : Stephen Howell

Age : 32

Works for : Microsoft, kinnectforscartch

Address : Old Coach Road,

Stonehouse,

Drogheda,

Co. Louth.

**Email :** v-sthowe@microsoft.com

stephen@saorog.com

**Phone :** Text 08722\*\*59

**Social Links**

http://stephen-howell.tumblr.com/

https://twitter.com/saorog/status/164817193903730689

http://archive.is/scratch.saorog.com

http://artandcode.com/3d/presenters/stephen-r-howell

http://scratch.saorog.com/blog.php/index.php/about-the-author/

http://www.adverts.ie/member/comments/101510/page-4

https://plus.google.com/107284575888682528548/posts

https://pipl.com/search/?q=saorog&l=+Ireland&sloc=&in=6

**Wife Details:**

**Name:** [Aileen H](https://twitter.com/AileenH)owell

**Works for:** Gibtex Limited as CEO

**Maiden name:** Gibney

**Company address :** Townley Hall Road,

Tullyallen,

Drogheda,

Co. Louth.

**Social Links :** [www.bumpbasics.com](http://www.bumpbasics.com)

https://plus.google.com/113517759738203788060/about

<https://twitter.com/AileenH>

<http://www.independent.ie/regionals/droghedaindependent/news/aileen-is-the-mastermind-behind-cheeky-maternity-wear-27101640.html>

http://www.bumpbasics.com (041-6862815)

http://www.magicmum.com/phpBB/viewtopic.php?p=172908&sid=d3fe645a21b6656b047ae1fa93e6e7a6

<http://ie.linkedin.com/in/aileenhowell>

https://www.facebook.com/aileen.howell

Children

## Sons : Jack Howell Age : six

**Son :**  Sam, who is 23 months old

## Daughter : Charis (four) Baby Sam,

## Daughter : Aileenhe new baby due in August.

Parents of 4 young children. D

**All Attend :** St. Joseph's C.B.S. Primary, Drogheda

**Clubs :** http://tweettunnel.com/coderdojodrog

<http://www.independent.ie/regionals/droghedaindependent/localnotes/planning-in-mid-louth-planning-in-mid-27122153.html>

# 

## There address to company address

https://www.google.ie/maps/dir/Townley+Hall+Rd,+Co.+Louth/Mary+Brennan+Designs%7CJewelry+Designer,Handmade+Jewelry,Unique+Jewelry,+Old+Coach+Road,+Stonehouse,+Dunleer,+Co.+Louth/@53.7793766,-6.510186,12z/data=!3m1!4b1!4m13!4m12!1m5!1m1!1s0x4867381f4dfbfcff:0x97a01ddcc5306b1e!2m2!1d-6.4329302!2d53.7351921!1m5!1m1!1s0x48673402d77ed8a1:0xd7b9b73f29410317!2m2!1d-6.394203!2d53.830035

## About Gibtex

Gibtex Limited is a family run company established over 20 years ago to meet the uniform and protective clothing needs of professionals. Over the years we have developed a range and in depth knowledge of the field and our experience is unique.

Gibtex was founded by Liam Gibney, a qualified Textile technician with years

of experience of every part of the textile chain - there's not much Liam didn't

know about fabric and how to meet the specific requirements of his

customers. Liam served on a panel of experts making recommendations to

Brussels about safety requirements in textiles. Since Liam's passing in Feb

2012 his family has continued to run the business whille striving to continue

to meet his very high standards.

From Fire Brigades to Marching Bands and Security Companies to Schools, Gibtex can meet their needs and offer a very competitive service at a price that offers the very best in value. If you would like to discuss your uniform needs with us please call us on +353 (0)41 9836701