Online Reputation Management

1. **Fake Reviews / Negative Reviews**

    a. Trip Advisor
    b. Google

2. **You Tube Videos**

3. **Social Networks**

    a. Facebook comments / impersonation pages / protest pages and groups etc
    b. Twitter comments / impersonators etc
    c. Hacked accounts

4. **Cyber Squatting, Passing Off and Abusive Domain Name Registrations**

5. **General Scam Warnings**

1. Fake Reviews and Negative Reviews

For the purpose of this document we are going to assume that the vast majority of business's we are dealing with on the island are holiday related business, i.e. B&B's hotels, self catering accommodation etc. and will therefore look in detail at Trip Advisor as the main review website.

We will look at google as well, on which any type of business can be reviewed.

Trip Advisor

If you google 'fake reviews on trip advisor' there are around 15 million search results returned. One of the top results is about a BBC investigation into fake reviews on the site and about half way down the first page of google is this site http://real-tripadvisor-reviews.com/ which offers to write reviews on trip advisor for you for $20 , there is a whole industry based on writing fake reviews on Trip Advisor!

The unfortunate truth is that anyone can write a review on trip advisor including your competitors, internet trolls and real customers.

If you go to trip advisors home page at http://www.tripadvisor.co.uk and type 'Isle of Wight' into the search bar it tells you they have over 1500 locations from hotels to restaurants to attractions with over 90,000 reviews combined. (make sure you are looking at The Isle of Wight in the UK, there is also an Isle of Wight in Virginia USA)

Anyone can leave a review on trip advisor whether they have really been to your property / restaurant / attraction or not.

As an example go to http://www.tripadvisor.co.uk/Hotel_Review-g190926-d6279723-Reviews-Riviera_B_B-Ventnor_Isle_of_Wight_England.html which is the trip advisor review page for The Riviera B&B in Ventnor, then click on the "Write a Review" button, this opens the review page that you or any of your visitors can then complete. Once the form is completed the person filling in the form has to either sign in or sign up but it's just a simple user name and email process, no real checks to see if you are a real genuine reviewer or not.

When you get to the end of the review there is a disclaimer to tick which states

"I certify that this review is based on my own experience and is my genuine opinion of this hotel, and that I have no personal or business relationship with this establishment, and have not been offered any incentive or payment originating from the establishment to write this review. I understand that TripAdvisor has a zero-tolerance policy on fake reviews".

This also has an info button that you can click which gives the following further info:

"TripAdvisor wishes to ensure that reviewers are not affiliated in any way with the establishment they are reviewing. By checking this box, you certify that you are not employed by the establishment, are not related to anyone employed there, and do not otherwise have a business or personal relationship with the owners or managers of this establishment or a competitor that might bias your review. In addition to being a violation of our terms of service and an unethical practice, committing fraud on reviews is also prohibited by the law and regulations in many jurisdictions [see (UCP 2005/29/EC) and (FTC 16CFR Part 255)]. Please see our Content Integrity Policy for more information."

It is not beyond imagination to assume that based on the fact that anyone can leave a review on trip advisor that potentially anyone with a grudge could write a fake or negative review causing damage to your reputation.

So What Can You Do About It?

Trip Advisor have a policy for reporting fake reviews.

On each review there is a tiny little picture of a flag, a very very tiny picture of a flag, if you click on that flag it opens up a pop up that you use to report the review with options such as:

Review Violates Guidelines
Review is Suspicious

Then more options when you click on one of the above such as:

Review Written By Competitor
Property Offering Incentives etc

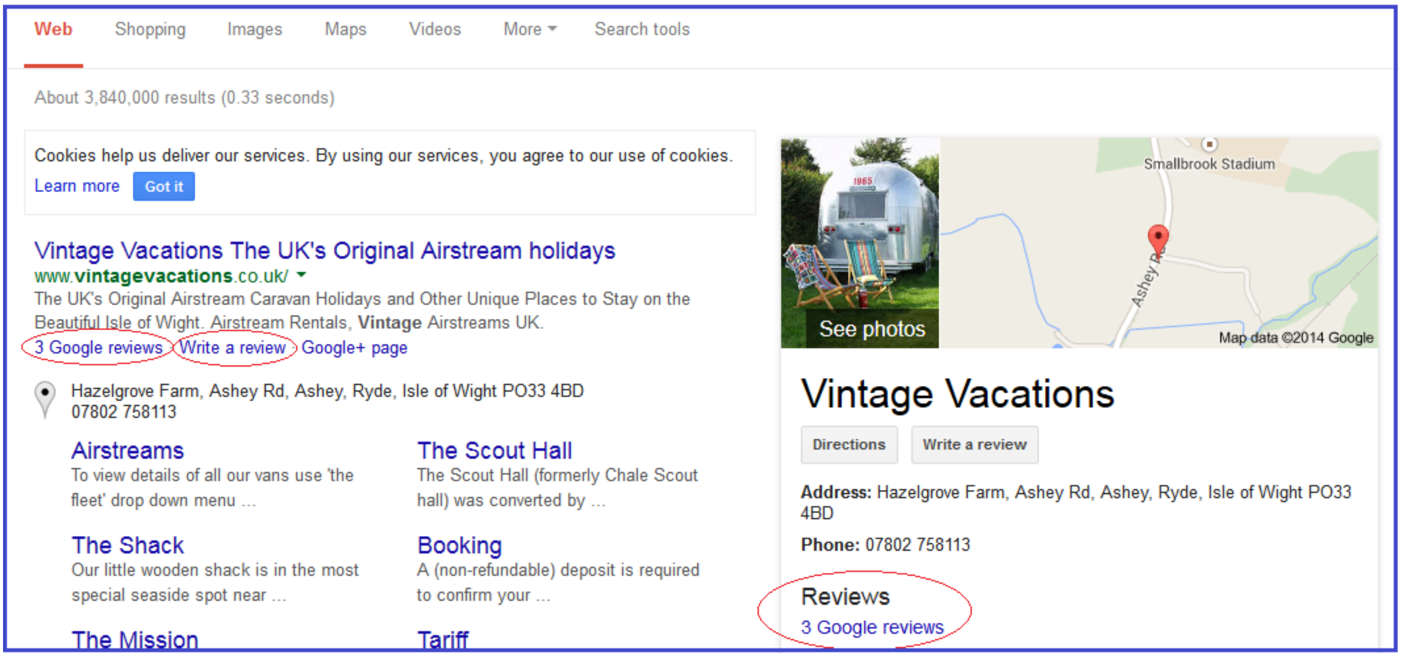
Then once you have selected the appropriate option there is a short info form to fill in. You only get 500 characters so you need to be quite specific and precise with the info you put in.

Trip Advisor have a help page with links to various reporting questions here
http://www.tripadvisor.co.uk/pages/fraud.html

It is also possible to contact Trip Advisor directly by going to
http://www.tripadvisor.co.uk/GeneralSupport

Google

Search for your business on google and if your business has been added to google places you should find the google map and address details come up on the right hand side of the screen, for example google ‘Vintage Vacations’ and you will get something like the result below.



About 3,840,000 results (0.33 seconds)

Cookies help us deliver our services. By using our services, you agree to our use of cookies.

Vintage Vacations The UK's Original Airstream holidays
www.vintagevacations.co.uk/
The UK's Original Airstream Caravan Holidays and Other Unique Places to Stay on the Beautiful Isle of Wight. Airstream Rentals, Vintage Airstreams UK.
3 Google reviews · Write a review · Google+ page

Hazelgrove Farm, Ashey Rd, Ashey, Ryde, Isle of Wight PO33 4BD
07802 758113

Airstreams
To view details of all our vans use 'the fleet' drop down menu ...

The Scout Hall
The Scout Hall (formerly Chale Scout hall) was converted by ...

The Shack
Our little wooden shack is in the most special seaside spot near ...

Booking
A (non-refundable) deposit is required to confirm your ...

The Mission

Tariff

Vintage Vacations

Address: Hazelgrove Farm, Ashey Rd, Ashey, Ryde, Isle of Wight PO33 4BD

Phone: 07802 758113

Reviews
3 Google reviews

The result returned by google will show you how may reviews the business has or if it does not yet have any reviews there will be a button that says ‘Be The First To Write a Review’, there will also be a ‘write a review link’ in the listing result.

Just like Trip Advisor any man, women or beast can write a review on google and again there is a whole industry based on people selling fake reviews, for example if you google ‘buy google reviews’ there are over 400 million results !

The only thing you need to write a review on google is a google plus or Gmail account and as soon as you log in you can write your review and any man women or beast can sign up for these.

So What Can You Do About It

Google have a help page here https://support.google.com/business/answer/4596773?hl=en which gives advise on how to report reviews.

They also have a form here https://support.google.com/legal/troubleshooter/1114905?hl=en which can be completed so that you can ask for content to be removed.

A word of warning though, google is a massive beast and they can often take some time to reply or to take any action.

2. YouTube Videos

Video cameras are everywhere, on phones, ipads, literally everywhere, and many many times people have ended up showing themselves up and being published on you tube for the whole world to see and judge. As well as this there are certain people that will make you tube videos purely for the purpose of damaging your reputation whether they hold a grudge or they are what is known as an ‘internet troll’, youtube is littered with examples of reputation damaging videos.

So What Can You Do About It

You tube is owned by google so when you are reporting content that you want to be removed from you tube you are basically going through the same process again of reporting to google.

You tube have a page here where you can start the reporting procedure https://www.youtube.com/reportingtool/legal?rd=1

They also have a ‘Privacy Complaints Procedure’ which states:

“If a video contains your personal information without consent, including your image, name, or national identification number, please contact us through our Privacy Complaint Process.”

The page can be accessed here https://support.google.com/youtube/answer/142443?hl=en

3. Social Networks

Online reputation attacks on social networks can range from negative comments on the various social networks to campaign pages to accounts impersonating your business and so on.

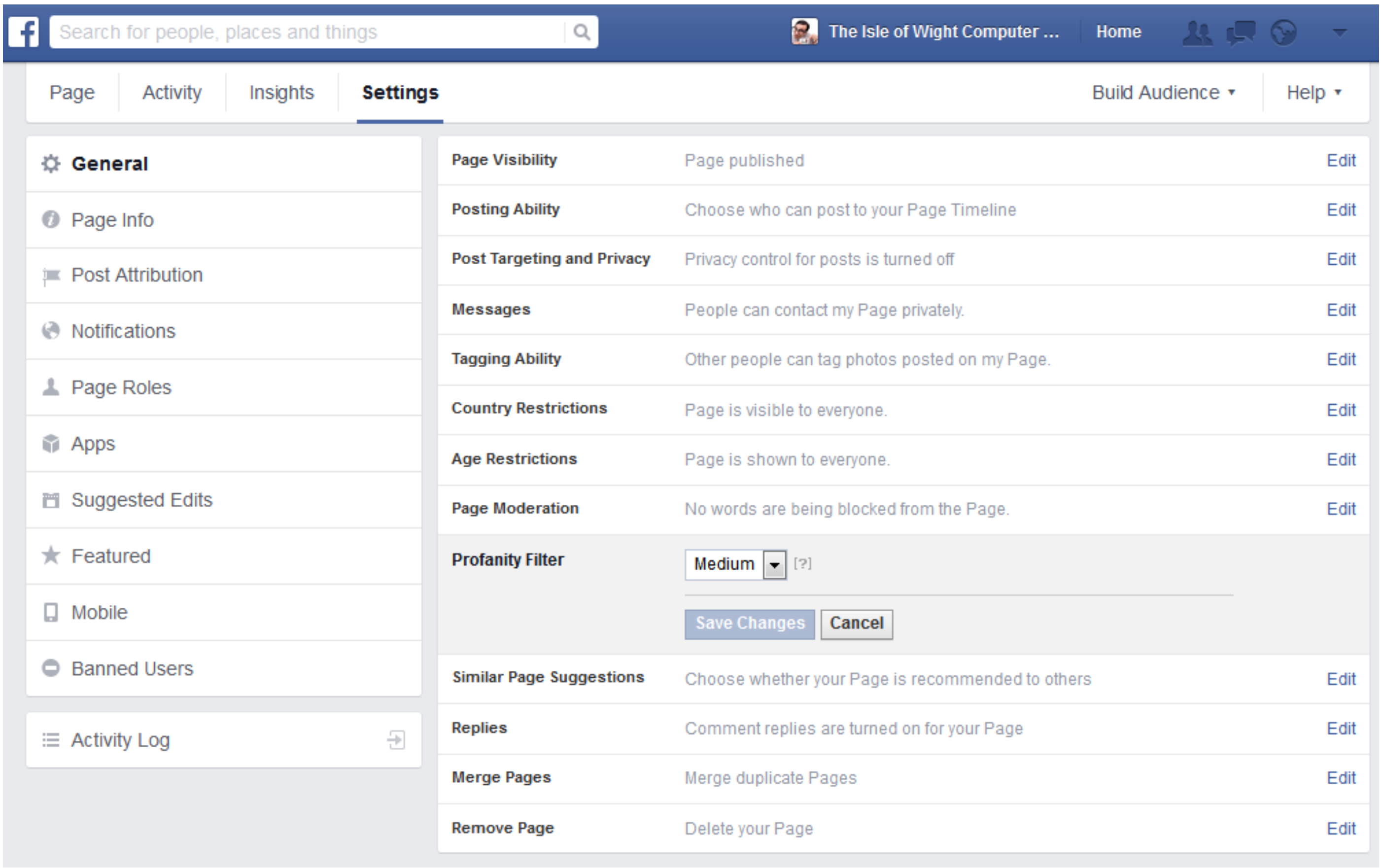
For the purpose of this document we are going to look at just facebook and twitter although there are many other social networks such as pinterest, linkedin etc that you should be just as vigilant with.

Facebook

Privacy Settings

Within the settings of your business facebook page you can set up things like a profanity filter to stop people posting bad language on your page and various other privacy settings and filters.

To get to these, log into your business facebook page then click on ‘Settings’, you will then get a page that looks something like this:



Page Visibility	Page published	Edit
Posting Ability	Choose who can post to your Page Timeline	Edit
Post Targeting and Privacy	Privacy control for posts is turned off	Edit
Messages	People can contact my Page privately.	Edit
Tagging Ability	Other people can tag photos posted on my Page.	Edit
Country Restrictions	Page is visible to everyone.	Edit
Age Restrictions	Page is shown to everyone.	Edit
Page Moderation	No words are being blocked from the Page.	Edit
Profanity Filter	Medium ▾ [?] Save Changes Cancel	
Similar Page Suggestions	Choose whether your Page is recommended to others	Edit
Replies	Comment replies are turned on for your Page	Edit
Merge Pages	Merge duplicate Pages	Edit
Remove Page	Delete your Page	Edit

It is worth just clicking through all of the settings in turn and making sure you have things set to a certain standard, some of the settings I would recommend are:

1. Make sure the profanity filter is turned on
2. Disable posts by other people on your time line (people can still like and comment but just won’t be able to post spam)

3. In the ‘Notifications’ setting make sure it is set to notify you each time there is activity on your page, this way you are alerted to all comments and can re-act to anything potentially damaging straight away.

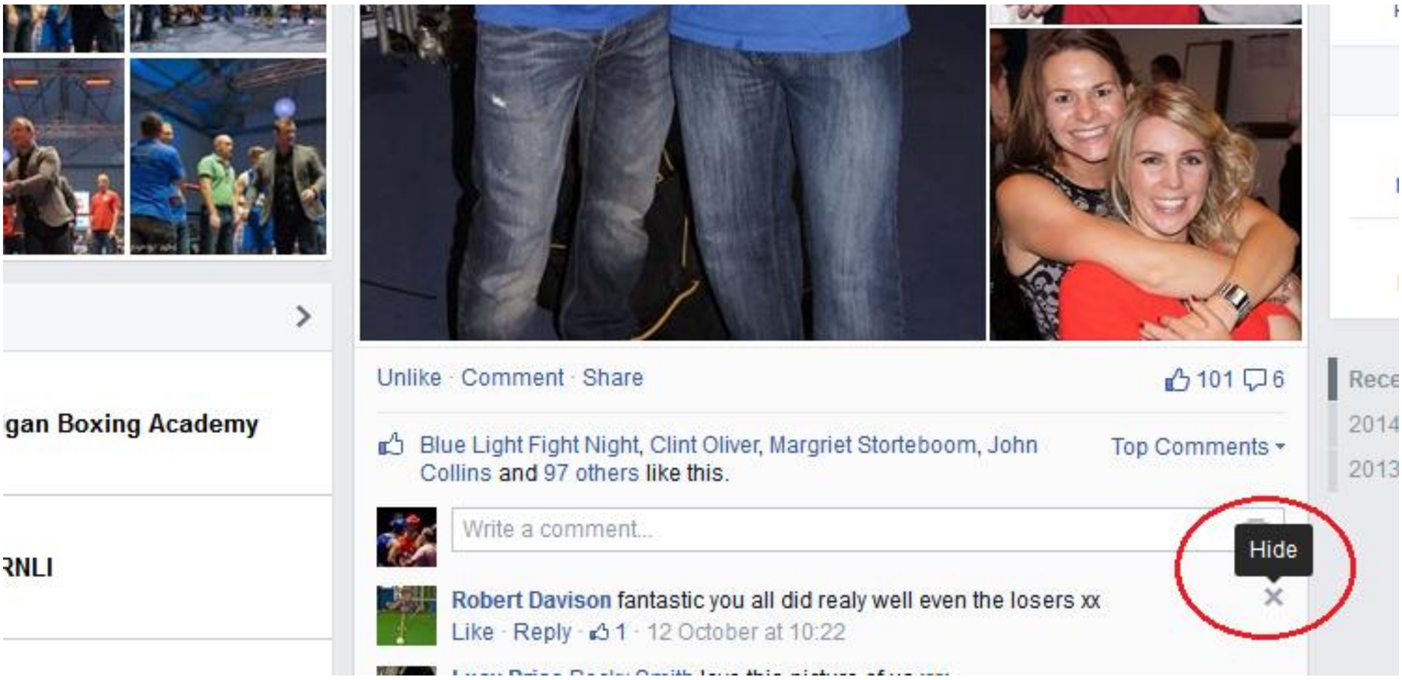
Security

As with all accounts that you have to log into it is very important to make sure you are using a secure password to deter hackers from taking over your account but with facebook you can also set up what is called ‘log in notifications’, which means you get an alert by text each time your account is logged into but you can also set up what is called ‘log in approvals’ which adds an additional layer of security to your facebook page by requiring you to enter a unique constantly changing code number when you log in which gets sent to your mobile phone, you can set this up on this page here https://www.facebook.com/settings?tab=security and it is worth doing to keep the hackers and trolls out of your account.

Removing and Reporting Offensive / Spam Comments

If someone posts any kind of offensive, defamatory or spam comment on any post you have added to facebook you can remove it and report it really easily.

Simply hover your mouse over the right hand side of the comment and a little popup will come up saying ‘hide’ (see image below)



Blue Light Fight Night, Clint Oliver, Margriet Storteboom, John Collins and 97 others like this.

Robert Davison fantastic you all did realy well even the losers xx
Like · Reply · 1 · 12 October at 10:22

Click on the little cross underneath the word ‘hide’ and the comment will be hidden from view.

You will then get offered other options including:

Unhide · Delete · Report · Ban

Click on any of those options to take the necessary action.

Someone Impersonating Your Business or Brand

If someone sets up a facebook page and pretends to be you or your business or brand you can report the details to facebook here https://www.facebook.com/help/contact/?id=208282075858952

Abuse, Harassment or Hacked Facebook Account

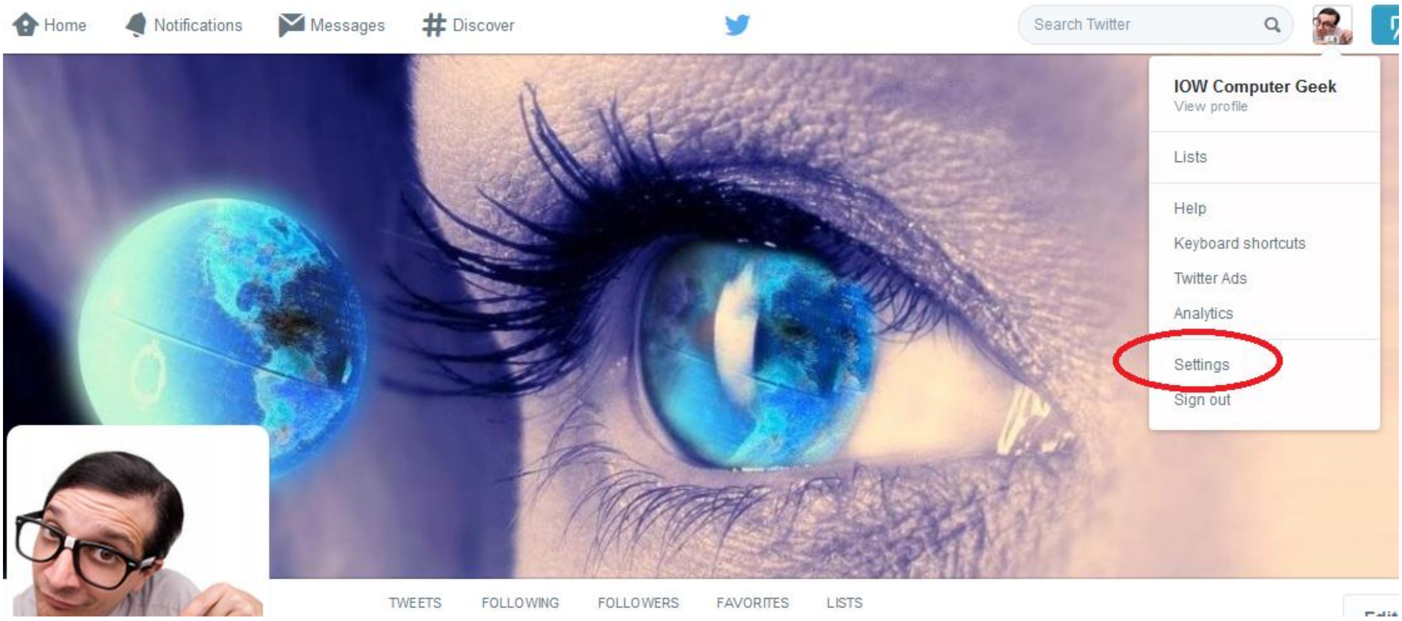
These can also be reported on this page https://www.facebook.com/help/contact/?id=208282075858952

Twitter

Twitter has many of the same settings as facebook which you can use to protect your privacy, security and reputation.

Privacy and Security

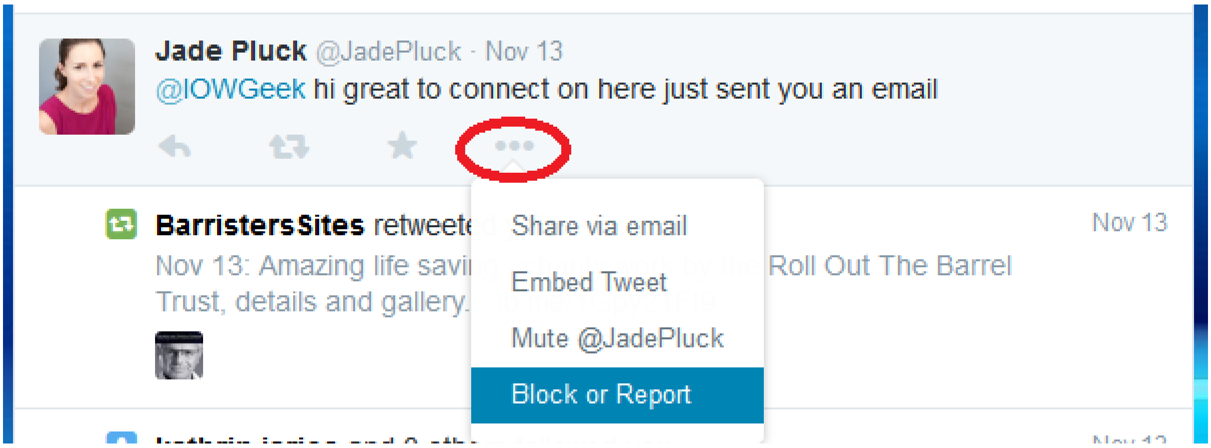
To access your privacy and security settings in twitter hover over your profile image icon in the top right hand side and then click on 'settings' (see image below)



In the security and privacy setting you can set up 'log in verifications' where you get a random code number text to you to each time you log in, this is a good way of keeping the hackers out but the first line of defence is to ensure you are using a good secure password.

Reporting Offensive / Spam Comments and Messages

If someone posts something offensive and references your user name in it you can report this by clicking on the three little dots underneath the comment and this will bring up various options that you can click on. (see image below)



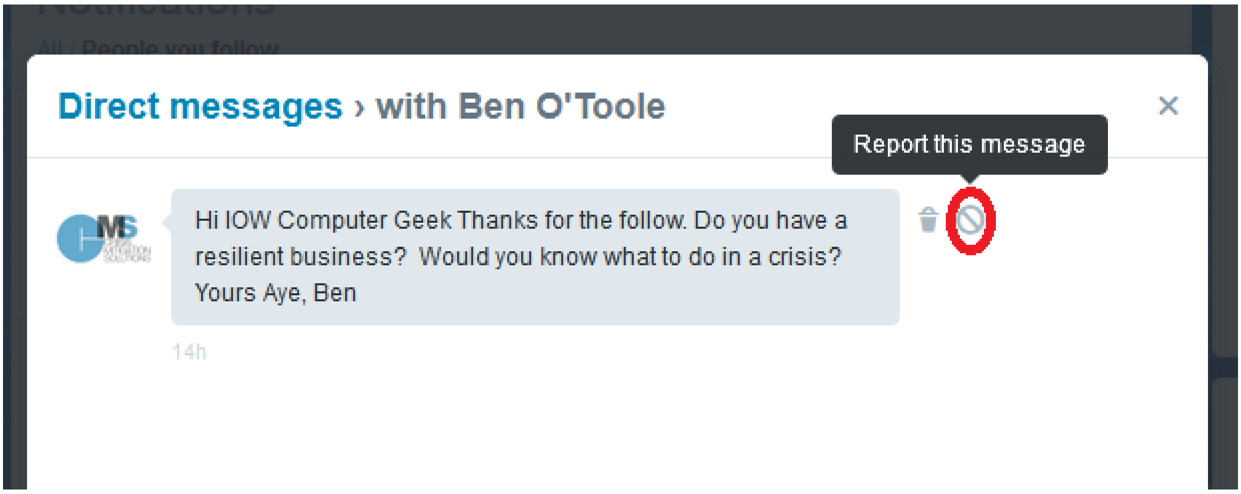
Jade Pluck @JadePluck · Nov 13

@IOWGeek hi great to connect on here just sent you an email

BarristersSites retweete… Nov 13

Nov 13: Amazing life savi… Roll Out The Barrel Trust, details and gallery.

In a similar way if someone sends you a direct message that is offensive you can report this by opening the message and clicking on the little icon that looks like a national speed limit sign and this will allow you to report it. (see image below)



Direct messages › with Ben O'Toole

Hi IOW Computer Geek Thanks for the follow. Do you have a resilient business? Would you know what to do in a crisis? Yours Aye, Ben

14h

Someone Impersonating Your Business or Brand

If someone is impersonating your business or brand on twitter you can report it by going to this page https://support.twitter.com/forms/impersonation

Twitter Account Hacked or Compromised

You can use the same page to report your account having been hacked or compromised https://support.twitter.com/forms/impersonation

Reporting Abuse and Harassment

To report abuse or harassment either directed at yourself or at anyone else you can use this page on twitter https://support.twitter.com/forms/abusiveuser

4. Cyber Squatting and Passing Off

This information is copied from http://www.findlaw.co.uk/law/criminal/crimes_a_z/500557.html

The term cybersquatting derives from the premise that individuals buy up certain internet domain names over the internet for a brief period before selling them on. This is seen as 'squatting' and is controversial because cybersquatters will generally target domain names that are sought-after by well-established businesses, which will then be forced to buy the domain names at a premium.

For example, 'Company A' is a well-established and famous brand but it does not yet have an internet domain name. A 'cybersquatter' has anticipated the company's need for a domain name and has bought all suitable names such as www.companya.com or www.acompany.com The company is now forced to either buy the domain name at a much higher price from the squatter, or purchase a different domain name that is not as easy to remember or relevant to Company A.

Cybersquatting is seen as immoral to certain people because the squatter has done very little to earn his money. His contribution has not helped society in anyway and has merely raised the cost for a legitimate company to buy a domain name. This problem in terms of domain names was particularly prominent in the early 90s with the explosion of the internet, as many major companies did not have domain names at the time.

Nowadays, a more concerning problem is individuals buying certain domain names which would make people think they are related to a certain company when in fact they are not.

Disputing Domain Names

In terms of disputing a domain name there are several likely complications or restrictions. Firstly, if the website host is not in the UK the UK courts may not have jurisdiction and thus power to bring a claim against the individual. There is also the possibility that the alleged cybersquatter could legitimately be using the website for its own purposes and just happens to have a similar name to that of another company. Even if it does not, if the website is not designed to take advantage of the company, and is not claiming to be affiliated to the company, it may be a reasonable use of the domain name, such as a dedicated fan site. However, if cybersquatting is clearly taking place an individual or company may be able to bring a claim for 'passing off'.

Passing off

In order to bring a claim for passing off, an individual or company must show it has built up sufficient 'goodwill' that an average individual would actually know who that company or individual was. If the cybersquatter has created a website with the domain name relevant to a legitimate company and the site is likely to lead to consumers believing it is the company's official site, and subsequently a loss is suffered, then a claim can potentially be brought. This type of claim can stop those cybersquatters which use obvious domain names for companies and then try to make money through that domain name and the firm's reputation.

Cybersquatting can be complicated and may come in a number of different forms. The old-style cybersquatter who jumped in quickly, anticipating a firm's success and hence the opportunity to sell on the domain name, may be being diminished, but there are still several cases in which individuals will use similarly named websites in an attempt to make money out of them. It is important therefore to know about cybersquatters and how you may be able to protect yourself from them.

Reporting Abusive Domain Name Registrations (UK)

Visit Nominets website at http://www.nominet.org.uk/disputes/resolving-domain-disputes/drs-guidance/abusive-registration

5. General Scam Warnings and Security Advice

The following are a range of general ongoing scams that anyone with an online business or online presence should be aware of and a bit of security advice.

Search Engine Submission Scam

Many owners of newly registered domain names will, usually within a day or two of registering their domain name, receive a strongly worded email / emails warning them that they must submit their new domain name to the search engines such as Google, Yahoo and Bing. These emails are usually worded in such a way that they make you think this is something you MUST do right now or you may lose out.

When you click on the link in the email you are then taken to a page that tells you with even more urgency how important it is to submit your domain name to the search engines and at this point you are usually invited to fill in a form and then pay a fee, anything from $90 to several hundred dollars for something that can be done for free!

More details on this scam at http://www.iowgeekblog.co.uk/search-engine-submission-scam/

Phishing Scams

Phishing scams work by trying to get the recipient of a fake email from a bank, mobile phone company, facebook, PayPal etc to visit a fake website where you are invited to enter your log in details, at this point the scammers then have your log in details and are then able to get into your real accounts.

More information on Phishing scams here http://www.iowgeekblog.co.uk/?s=phishing

Emails with Virus Attachments

Full details on recent emails with virus attachments here http://www.iowgeekblog.co.uk/?s=virus

Microsoft Telephone Scam

Full details on this scam here http://www.iwcp.co.uk/news/news/microsoft-telephone-scam-hits-the-isle-of-wight-45598.aspx

Using Secure Passwords

Advice on password security here http://www.iowgeekblog.co.uk/keeping-your-content-manged-website-happy/