Internet Security Issues

Purpose:	To provide guidance for barristers on the potential internet security risks associated with social engineering (phishing) and domain name hijacking.
Scope of application:	All practising barristers and chambers
Issued by:	Information Technology Panel
Last reviewed:	July 2020
Status and effect:	**Please see the notice at the end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

Social engineering (aka phishing)

1. It is unfortunately common nowadays for criminals to use what are known as social engineering attacks to obtain personal information which they can use for their own purposes. There are various types of attack: making a telephone call to find out seemingly innocuous information (don't give the information, just say you'll call the bank/whoever directly to confirm it, and use the number on your statements!); sending those enticing e-mail invitations inviting us to help recover large amounts of money, providing we give the recipient our bank details; and bogus web sites that look like the online bank or online service we always deal with, but are, in fact, collecting our pass-words and identity details in order to enable the malefactor to access bank or credit card accounts, or other information. We may be familiar with these modes of attack, and the software vendors do try to make it more difficult for attackers to spoof a web site, for instance.

2. However, despite the valiant attempts by service providers, the nefarious are well-versed when it comes to using technology to their advantage and the target is not

always financial information. Although the vast majority of phishing attempts are straightforward attempts to get at bank accounts and credit cards, sent en masse to auto-generated email addresses, there are increasing examples of specifically targeted phishing attempts which are sent to particular individuals, with the aim of getting passwords to email accounts in order to be able to access information likely to be held in those accounts (such as security information, government information, or commercial information).

3. These specific attempts are generally known as spear phishing, or whaling, and will often have involved some work to gather personal information about the target to try and increase the chances of success – and may well succeed. They work on the basis that if a scam email already contains some of your personal information, or appears for example to come from another member of chambers or a solicitor who regularly instructs you, or perhaps mentions a case you have appeared it, you are much more likely to think it is genuine. Particularly effective emails seeking to extort money from people have been circulated recently, claiming to prove that they were genuine by referring to the recipient's passwords. They took advantage of the fact that many insecure passwords associated with particular email addresses have been revealed in past data breaches and are available at several places on the internet. The recipients, however, thought the emails were genuine, because they did not realise that their passwords had been made public. In a training exercise at a US military academy, 80% of those sent an email which appeared to come from a senior (non-existent) officer clicked on a link in the email which specifically requested personal information.

4. If you get an email asking you to – for example – verify your account somewhere: don't click the link in the email, but instead contact the company (bank, etc) by telephone (don't use any numbers in the email, which may well be fake and will be answered by one of the criminals' associates) and check with them, or go to the website in your browser (type in the address you know to be real – don't copy it from the email) and check your account that way.

5. In the business world there has been a recent spate of emails to junior employees or financial controllers purporting to come from their boss and asking for money transfers to be made urgently because some particular deal is about to be closed. Solicitors have been asked to transfer sums owed to their clients in a particular case to a criminal's bank account on the pretext that the "details have just been changed" – the criminal found out the relevant details by hacking into the client's email accounts and using the information found there to impersonate the client to the solicitor. Watch out

for emails asking you to transfer money, or refund fees. If you are in any doubt at all, phone the person concerned and check that everything is as it should be. It may be sensible to warn Chambers staff members who deal with fees to be aware of these types of attacks if your Chambers' staff training has not covered it.

6. Also be careful of links to apparently real website addresses: slight tweaks can mean you end up on a fake site, and the fake sites can appear practically indistinguishable from the real thing – a lowercase letter L or O may be replaced with a number one or zero, for example. A few years ago, the security service G4S (g4s.com) had their website spoofed at g4s-plc.com, with the addition of a fake press release with a profit warning; the result was a drop in share price. The purpose there was to attack G4S via media manipulation, but the same type of tweaked address could be used to fool people into thinking they were on a legitimate website. It's not just the part of the name before the dot that can change: the proliferation of top level domains ('TLD's – such as .com, .org, .net, .info, .name, .london, .tv ... and many many more) means that businesses may not have acquired all of the relevant TLDs. Be careful before you log into something to make sure that the address really is right.

7. Remember also that an email which appears on its face to have been sent to you by someone you know may in fact be from an impostor, as it is possible for an impostor to conceal their real email address. You can check the sender's real email address by opening the email, clicking on File, Properties and then examining the Internet Headers.

Domain name hijacking

8. Domain tweaks are used to create fake websites to get personal information, but can also be used to trade off an established business name – hoping to get business by confusion – or to attack the business (as in the case of G4S, above). In some cases, the domain may even be hijacked, when someone fraudulently takes control of a domain name, often by masquerading as the legitimate administrative contact for a domain name. In both cases, the damage inflicted can be significant. One barrister had their domain name misused in this way, and defamatory material posted on the hijacked web site, much to their distress. This matter took some time to deal with, and they had to take specialist advice and help from a firm of solicitors. The effect this had on their daily working life can only be imagined.

9. Setting a registrar-lock on your domain is one way to deal with this – it means that the account details cannot be modified via email; changing anything, including a transfer of the domain, requires logging into your account with the domain provider. Check with your domain name registrar how to do this – in practice, most registrars lock domains by default now.

10. If a tweak on your domain name is registered – or your website is copied/spoofed to another domain altogether – there are a couple of practical steps that you should take:

(a) First, if it's clear that there's some sort of scam being run using the web-site, contact Action Fraud (actionfraud.police.uk).

(b) In addition, consider contacting the FSA – not the most obvious thing in the world, but there's a chance that the fake website is there to support a scam that may come within the remit of the FSA. This is more likely with solicitors' firms than individual barristers or chambers, but not all faking comes from within the UK and the individuals setting up the site may not understand the difference. If there is a possibility that the website is set up to support a boiler room scam or similar, the FSA may well be interested and be able to lend support to any action to take the site down.

Copied content

11. What if someone copies and reuses all your lovingly crafted content? This can be material such as biographies etc, or articles and similar blog-type content. If the biographies have been used, treat it as potentially a fake website and consider reporting it to Action Fraud and the FSA. More often, the material is simply 'scraped' and copied onto a website that is used to try to get advertising money in. It's annoying but not usually malicious.

12. To get anywhere with dealing with fake content, the best thing to do is to complain to the hosting service for the site (find it using a 'whois' service – use a search engine to find one). Hosting services are the companies with servers that actually store the websites and display the pages when someone visits the website (by and large) – in most jurisdictions they aren't responsible for the content until they are notified that there is a copyright violation – so notify them. Most reputable hosting services will take down the content either immediately or after a short period of time, allowing the website owner time to take down the material directly.

13. Copyright infringements are a violation of Google's AdSense terms of service; there's a fairly good chance that someone who takes content from another website is looking for ad revenue, and may well have registered with Google to do so. The Google AdSense terms and conditions specifically require the website owner to warrant that the content on the website does not infringe on anyone else's intellectual property – reporting the violation to Google will, at least, hurt financially. Search for "AdSense report violation" to find the page for reporting violations. Other advertising systems have similar policies – look for an "Ads by ..." link somewhere around the ads on the site to see whether it's served by such a system.

14. On a similar note, report the website to search engines anyway – Google et al have procedures to remove material that infringes copyright (you may have to dig through their sites, or search for it). Removing the pages from search results will reduce visitor figures – it's not quite as helpful as getting rid of the site altogether, but it would reduce the impact of the copying.

15. If the domain is very similar to your own name, then it may be possible to use the Uniform Domain Name Dispute Resolution Policy procedures to prevent use of the problem domain.