House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Phishing Attacks – false ATO sites**
Hansard Page:	**COMM 3**
Question No:	**1**

CHAIR—I have one more question in relation to false ATO sites. I understand from your submission that, with the large increases in the number of people online, there has been some difficulty with fake ATO sites being set up and people going on and divulging personal information thinking it is the ATO. I understand there was a site being hosted in the Ukraine that was doing that. How prevalent is that and what is the ATO doing to try and reduce that risk or to protect people from that?

Ms Konti—I can answer that. The type of cybercrime that we are seeing more and more often around the tax office is in fact these phishing attacks, where there will be people who host sites that look like the tax office and offer a very credible tax office image that are specifically designed to lure taxpayers into providing personal information. When we discover one of those—and the discovery is either through AusCERT, a not-for-profit agency that we have partnerships with and they can sometimes alert us to these, through our own discovery mechanisms or in fact through having them reported to us by a member of the community— there is a security action plan that then gets kicked off as a result of that. We work with the AFP and the High Tech Crime Centre to basically identify the site and to shut it down. Then we have a number of communications mechanisms available to us through our website and through various media releases in order to be able to alert the community to this going on.

CHAIR—When you say shut it down, how do you do that if it is located in the Ukraine, outside the jurisdiction?

Ms Konti—I understand that we can shut down the site and prevent it from being able to be available. To find out exactly how that happens, I would have to take that away.

CHAIR—I would be very interested to know.

Mr Gibson—Each of the sites has unique network identifier and the High Tech Crime Centre, in conjunction with the internet service providers all round the globe, works to identify a network address that is doing this. They have a way of completely turning that off so that, even if the site is still trying to be active, it is denied access to the internet. That address is made invalid. We can get some better explanation for the committee on that.

CHAIR—I would very much appreciate that.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Answer:

The Tax Office uses the Australian National Computer Emergency Response Team (AusCERT) to shut down malicious websites. Typically, from when the Tax Office reports details of a malicious site to AusCERT it takes between one day and a week for the site to be shut down.

The Tax Office understands the task of shutting down malicious sites is very difficult as there are a number of factors to consider, for example, different jurisdictional legal requirements. This may mean that, depending on the relevant law in a particular jurisdiction that a web site is hosted, AusCERT will have varying degrees of success in shutting the site down. It is not uncommon that one or more similar phishing sites are activated when a site is shut down.

In some cases, the Tax Office is able to identify when a phishing site is using Tax Office web servers as part of its operation. For example, a phishing site may reference the Tax Office logo directly from an official Tax Office website. In such cases, the Tax Office is able to detect the unauthorised use of the logo and re-configure its web servers so that when the logo is referenced from the phishing site it will display a different image informing the user that they are visiting a phishing site.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Varying of ABN information**
Hansard Page:	**COMM 6**
Question No:	**2**

Mr BILLSON—With the ABN process, I imagine all that is ripe for simplifying some of that front-end regulatory requirement, but now those business entry points have a degree of overlap with other jurisdictions—whether you get your ABN, your register, your business and all these kinds of things. Has that highlighted any new challenges in terms of security of that information? In terms of other people using it, there is some suggestion that there is legislation that lets third parties vary their personal and business information under that collaborative arrangement. I am just wondering whether you have had any experience or observations about that.

Ms Konti—The Australian Business Number is a little bit different to the tax file number in that it is a public number. There is a lot of publicly available information that is connected with an ABN that is available to all of us to look up through the Australian Business Register site.

Mr BILLSON—There is a suggestion that others can vary the information that sits behind the ABN and there are questions as to whether you are an organisation that has the scope to vary the information or whether there are others who can impact on that information other than the person to whom the number was issued.

Mr Gibson—What we might do with that one, given that it seems fairly complex, is we might take that on notice and come back with an expanded response on that particular question.

CHAIR—We would appreciate that.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Answer:

Provided that proof of identity requirements have been satisfied, a business can update most of its own details using one of the following methods:

- online via the internet
  - using the Australian Business Register (ABR) at: www.abr.gov.au
  - using the Australian Government Business Entry Point (BEP) at: www.business.gov.au
  - using the Tax Office Business Portal at: bp.ato.gov.au (information is exchanged between the Tax Office's system and ABR)
- through the tax agent electronic lodgment system (ELS)
- by phone, email or facsimile to the ABR
- by submitting a change of registration details form or a signed letter containing the necessary information to make the change to the Australian Business Registrar, or
- by lodging any Tax Office transactional form that provides for the update of details.

Updates to data on the ABR can be made by the authorised contact person(s) named on the ABR (including tax agents where they are an authorised contact). The ABR may also be updated when relevant data updates flow from Tax Office systems to the ABR, for example, when a business updates its postal address on the Tax Office business portal the business's record on the ABR is in turn updated automatically.

The Tax Office uses certain third party agency data to validate information at registration and subsequently to maintain the integrity and currency of data on the register. These agencies include the Australian Securities and Investments Commission, Australian Prudential Regulatory Authority and the Registrar of Births, Deaths and Marriages in each State and Territory.

Recent legislative changes authorise the Australian Business Registrar to update incorrect details on the ABR from any source where the Registrar believes that source to be correct. The Registrar is currently planning a data matching pilot as a first step towards implementation of these new provisions.

There are certain details that cannot be automatically updated online on the ABR including the legal name of a company and the legal name of an individual. These can only be changed by supplying evidence of a change to the Australian Business Registrar.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Timeliness in dealing with TFN abuse**
Hansard Page:	**COMM 11**
Question No:	**3**

Mr Cranston—In relation to the file number abuse, when there is suspected to be misuse of a file number or a stolen file number there are immediate inquiries. Often, if a particular person says, 'I haven't even lodged my tax return,' that matter can be dealt with very quickly. The file number will be locked down and a new file number will be issued immediately. I can take on notice the time that all takes. Timeliness is very important for that, so I think it does happen rather quickly.

Mr Gibson—We will take that on notice. There is another example in the last few years that I recall. A tax agent's premises were burgled.

Answer:

Where the Tax Office suspects a Tax File Number (TFN) either has been, or potentially is, compromised through misuse or theft, an indicator is immediately activated in Tax Office systems to prevent refunds from issuing.

The Tax Office has procedures in place to issue a new TFN where a TFN has been compromised. These procedures require the taxpayer to attend the nearest Tax Office shopfront with proof of identity documentation. The process for issuing a new TFN takes approximately six to eight weeks as additional checks need to be undertaken, including confirming the client's identity with third party organisations. The only limitation on the taxpayer's dealings with the Tax Office during this period is that no refunds will automatically issue until a new TFN has been issued. Where an application for hardship is approved, priority is given to expedite the repayment of the refund and the TFN replacement.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Standards and security for tax agents**
Hansard Page:	**COMM 11**
Question No:	**4**

Mrs HULL—You have just raised the case of the tax agent's office being burglarised. What specific standards and systems do you have in place for the registration of businesses like tax agents and what sort of security they have? Do you have a set of standards for the security measures that they have to have on their systems before they can be a tax agent? Is there a role for auditing these tax agents? What do they have to comply with in order to be able to deal with the tax office? What are the standards that they have to comply with? Is there an audit to ensure that those standards are being upheld?

Mr Gibson—I think there are two dimensions to that, and I am going to ask Michael to answer on one of them. In terms of the technology side of it, we have a Software Industry Liaison Unit, and we do a lot of work with developers of things like accounting practice management software. It is only those legitimate software packages that can interface with the ATO. Through that liaison unit, we have quite good engagement about standards and so forth. As to tax agents, in terms of certification, we do not certify tax agents, I do not believe. I think that is an accreditation that comes from a professional association. If that is not correct, I will come back, because I am an IT person rather than a tax person. But I am sure that is the case. So those professional associations have accreditation and quality assurance processes that they run within—

Mrs HULL—And that is in conjunction with the ATO? Do they have a set of standards to meet in relation to their connection with the tax office? Do you set out a set of standards that all of their members must meet?

Mr Gibson—I will need to take that on notice, unless Michael knows.

Mr Cranston—We will take it on notice.

Answer:

The Tax Office does not stipulate a set standard of security measures that a tax agent must employ in their practice. However, the Tax Office regularly communicates information about security issues and practices to tax agents through marketing and communication channels such as:

- The Tax Office website at: www.ato.gov.au
- A quarterly TAXAGENT magazine

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

- A Tax Office eLink weekly subscription email newsletter for tax professionals
- broadcasts (e.g. urgent email or paper communiqués sent to all tax agents)
- An annual Tax Practitioner's seminar, and
- Tax Practitioner webcasts.

The Tax Office does not actively audit tax agent security measures. However, when the Tax Office becomes aware of a serious breach of security concerning a tax agent's clients, the Tax Office will contact the tax agent with advice and provide assistance, such as replacing compromised tax file numbers.

The Tax Office has secure methods for tax agents to electronically interact with the office. For example, transactions transmitted from a tax agent's business practice software through the Tax Office's electronic lodgment service (enrolment via written request) are encrypted and sent through a secure connection. Tax agents use a combination of codes and passwords to assure the Tax Office that these transmissions are from an authorised and trusted source.

Tax agents, or their staff, who want to use the Tax Office's online services must first register for a digital certificate. The digital certificate is used to log in to Tax Office online services (such as the Tax Agent Portal or electronic commerce interface) to lodge transactions or access client records in Tax Office systems. Tax Office digital certificates use public key infrastructure (PKI) in line with the government's Gatekeeper PKI Framework strategy for use with government online services.

In addition, tax agents must obtain written authorisation from clients before submitting a return or activity statement electronically to the Tax Office on behalf of clients. Prior to transmitting a return or activity statement electronically to the Tax Office the tax agent must also electronically declare that they have obtained this authorisation.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Time taken to shutdown host websites**
Hansard Page:	**COMM 12**
Question No:	**5**

Mr GEORGANAS—I know that this is a hard question to answer, but how long would it take to shut that host website down?

Ms Konti—I would have to take it on notice. I think that it is very fast, but we did not come prepared for—

Mr GEORGANAS—I suspect the criminals then would go onto another host site.

Mr Gibson—Some of them are very sophisticated and just hop around, yes.

Mr GEORGANAS—In case of this last one, the bogus one, it was going around for a few months at least, I think.

Mr Gibson—We will include that and bring it back too.

Answer:

The time taken to shut down a website varies due to cross border issues such as legal issues, relationships between countries, language barriers etc. In the Tax Office's experience it can range from one day to one week.

Once a site is shut down it is possible that another phishing site is created in a matter of minutes. However, in most cases this would require another phishing email run to direct traffic to the new site.

For the financial year July 2008 to June 2009, there were 51 variants of the Tax Refund phishing scam. Upon investigating some of these phishing scams, the Tax Office found instances of scam websites that were not yet fully active but in the process of being prepared for future use.

Phishing scams are typically conducted in cycles with runs lasting anywhere from a few days to a few weeks. During our Tax Time period in early June 2009 to late July 2009, the Tax Office identified two to three potential new phishing web sites on a daily basis. This has since tapered to around one instance per fortnight.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Assisting taxpayers in relation to Cybercrime**
Hansard Page:	**COMM 13**
Question:	**6**

Mrs HULL—… Is there an ability to come back to us with information about what could be done to ensure that there is a strategy being worked up to deal with the people's perception of the ATO and whether or not you are trying to help them or hinder them? They stand to be more vulnerable, purely as a result of the feeling that the ATO are seeking answers from them and they need to respond straightaway…

Ms Konti—In relation to helping particularly in the cybercrime space, we will take that away and come back to you…

Answer:

To provide the community with confidence in and greater accessibility to the Tax Office and the tax system, we have developed corporate frameworks, systems and strategies that guide how we interact with our clients. This underpins all our activity, and contributes to the community perception that we are fair, professional and approachable in all our dealings.

As a large government agency providing many online services we continue to balance ease of online access and security for the community to interact safely. We have a number of education and awareness campaigns in place to increase recognition and protect and empower our community.

The Tax Office continues to monitor the environment and send consistent messages to the community about what we expect from them and how we establish our identity. We make it clear that our emails or SMS messages will never ask for your personal information such a credit card details, tax file number (TFN), date of birth or passwords.

The Tax Office also has a proactive media strategy and notifies the community immediately when it perceives they are at risk. For example, between January 2009 and November 2009 the Tax Office issued five media releases warning people to be wary of fraudulent emails. One particular release warned clients of an email circulating that claimed to offer a 30 per cent discount on their taxes. The media release was picked up a total of 85 times in the press, 48 times in television and 121 times on radio and seven times on the internet. It also resulted in a senior tax Commissioner being interviewed on three occasions, twice on ABC Radio and once for the West Australian newspaper. The approximate audience reach as a result of the coverage was around 1.3 million people.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Our most recent Community Perceptions Survey notes that 80 per cent of the community agreed with the statement that overall the Tax Office is doing a good job. More importantly, the survey notes that there was strong agreement that the Tax Office is there to offer assistance. Also, the survey indicates that the Tax Office is continuing to become more accessible and approachable with more people saying they are comfortable going to the Tax Office with problems, reflecting a continued increase in engagement with us. We continually assess community perceptions and are committed to monitoring and improving these strategies and addressing any perception issues.

The Taxpayers' Charter is our client service charter which sets out the commitments we make to the community and explains what people can expect when dealing with us. The Charter also helps us build community confidence in how we manage the tax system. It explains our relationship with the community – a relationship that is based on mutual trust and respect. By keeping people well-informed of their rights and obligations, and ensuring that we are fair, consistent and respectful in all our interactions, we are continuing to build taxpayer confidence and their perceived ability dealing with us on an equal footing.

The Tax Office Corporate Values guides our behaviour as a fair and professional administrator of Australia's tax and superannuation systems. We strive to demonstrate our corporate values in all our work and interactions with the community. This helps to build a trust in our relationships and provide a consistent experience for the taxpayer.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic: **Virtualisation software**

Hansard Page: **COMM 13**

Question No: **7**

Mr BILLSON—On page 6 of your submission you made some points about increasing vulnerability, and cloud computing was one that was raised—I can see the fiscal architecture opening that up. But you touched on virtualisation software. I imagined what that meant and did not get very far. I have tried to imagine a bit more and I think you mean Second Life and things like that where you can trade and transact. Is that what you meant? Because I did not know what 'virtualisation software' meant. I have just tried to fire up Second Life where you are in a 3-D virtual world. I know there is increasing commerce in these virtual worlds and I am wondering whether you are saying people might inadvertently provide personal details about themselves to engage in these activities. That is the best I could come up with. I have no idea what you meant. The bullet point I am referring to reads:

• paradigm shifts in the way IT is used, such as cloud computing and virtualisation software where new opportunities for cyber crime might occur

Mr Cranston—It would be really early for the ATO in this particular space, but we know these things exist and if you are talking about crime, potentially some of these sites are used as areas where you can trade and there is potentially income that should be taxed by the tax office, so that is probably one concern. I think there is also potential where profits or proceeds of some crime could be somehow laundered through that. That is not particularly a tax issue but tax fraud and then the laundering of it could become a tax issue.

Mr BILLSON—So I was on the right page generally with what you meant there.

Mr Gibson——We will take it on notice and if there are any other aspects to it we will provide that information to you.

…

Mr BILLSON—So beyond the cloud there is the architecture.

Mr Gibson—We will try and clarify that in plain English for you.

Answer:

Virtualisation software in the context of the Tax Office submission means emulation, through software, of a physical computer. Doing so makes it possible to mask any details of the actual hardware in use, therefore easily permitting machine anonymity. This software allows a mischievous user to configure and present misinformation,

thereby thwarting efforts by authorities to log, collate and analyse their actions and gather physical evidence to build a case against them.

There are other security concerns associated with virtualisation software including issues with portability, whereby entire systems can reside as a simple file thus making it easy to copy/steal the entire system including the data.

Virtual economies or virtual worlds (such as Second Life) are different concepts which have gained in prominence in recent years. The Tax Office continues to monitor developments in this area.

Cloud computing refers to the use of third party infrastructure which is accessible via the Internet. This can constitute computing services, software, internet protocol address, data storage etc. Generally, this infrastructure can be constructed and configured in any manner and changes made to it in real time from anywhere in the world.

Cloud computing also permits the aggregated use of computing power i.e. harnessing the power of multiple computers. As with virtualisation software, the significant issue is how these services are used. Cloud computing, coupled with the virtualisation software as described earlier, can provide a very useful platform to launch attacks overtly or covertly. Once again, the ability to detect, identify, log and analyse real information associated with such activity is difficult.

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

Inquiry into Cybercrime

16 September 2009

Topic:	**Tax Office engagement in the legislation**
Hansard Page:	**COMM 14**
Question No:	**8**

Mrs HULL—Was the tax office sufficiently engaged in the new identity fraud legislation that is in front of the House?
…

Mrs HULL—… what I am asking is: were you engaged in it? The question I am asking is: were you asked? Was the tax office asked to engage in this legislation?

Mr Cranston—I will take that on notice. Sometimes with legislation like this, if it is relevant to the ATO we are asked for a response. But I do not know if we were engaged in this particular legislation.

Mrs HULL—The second question, if you would take it on notice, is: if you were engaged, do you think the offences in the legislation are broad enough to capture the concerns that the ATO might have?

Mr Cranston—Yes, I will take that on notice.

Answer:

The Tax Office presented a submission in response to the discussion paper on Identity Crime which was circulated in 2007 by the Model Criminal Law Officers' Committee of the Standing Committee of Attorneys'-General, which is available on the Attorney-General's website.