Australian Government
Australian Taxation Office

PO Box 900
Civic Square ACT 2608

Ms Cathyrn Ollif
Committee Secretary
Joint Select Committee on Cyber-safety
Department of House of Representatives
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Ms Ollif

The Australian Taxation Office (ATO) welcomes the opportunity to make this submission in response to the House of Representatives Committee inquiry into Cyber-safety for Senior Australians.

The ATO has adopted a proactive approach to cyber-safety and has a range of systems and strategies in place to protect our clients. We have also developed a focused capability to detect and respond to scams. This has been spurred by the fact that the ATO is often the subject of scams due to our extensive interaction with the community and the community's willingness to comply with requests from the ATO. Scammers utilise this unique position of the ATO and its brand to play on the public's confidence and legitimacy of our authority.

Our submission details:

- How we detect, manage and respond to cyber scams.
- Some of the trends we are witnessing in terms of the increasing prevalence and sophistication of cyber scams.
- How we are informing and educating the community about scams, online security and how to interact safely with the ATO.
- Suggestions for how other organisations can participate in creating a culture of online security awareness.

We trust that our submission will be a valuable input into the inquiry. I, along with Todd Heather (Chief Technology Officer), will be happy to answer any questions at the Hearing or out of session.

Yours sincerely

Bill Gibson
Chief Information Officer
Australian Taxation Office
16 May 2012

ATO Submission to House of Representatives Committee on Inquiry into Cyber-safety for Senior Australians

Introduction

1. The Australian Taxation Office (ATO) welcomes the opportunity to make this submission in response to the House of Representatives Committee inquiry into Cyber-safety for Senior Australians.

2. The ATO has adopted a proactive approach to cyber-safety and has a range of systems and strategies in place to protect our clients. To date, our focus in cyber-safety has been directed towards all clients rather than any particular demographic group.

Summary

3. The ATO notes that information and communications technologies are a part of the everyday life of doing business. Over the past decade, there has been a conscious direction to increase the utilisation of the online channel in conducting business. While the complex and ubiquitous nature of the Internet can seem daunting, the ATO has not lessened its efforts to utilise this channel in seeking efficiencies around service delivery.

4. The ATO is often the subject of scams due to our extensive interaction with the community and the community's willingness to comply with requests from the ATO. Scammers utilise this unique position of the ATO and its brand to play on the public's confidence and legitimacy of our authority. This is not dissimilar to the use of the various bank brands in related scams. As such, the ATO has developed a focused capability to detect and respond to scams, which complements its IT Security Incident response function. This has allowed the ATO to better manage and respond to such events in an agile and timely manner. This will continue to be so.

5. Correspondingly, the ATO understands that a greater level of commitment is required in protecting classified information including sensitive, financial and personal data. The reality is that cyber crime has grown significantly alongside the growth in legitimate online business and commerce. A vast underground economy now exists, which provides all the tools of trade to facilitate such activity, including a market for transacting in such data.

6. The ATO responds to these risks and threats in various ways which focus on the Australian public, inclusive of senior Australians.

7. The ATO first became aware of an ATO branded phishing e-mail in 2007. Since then the sophistication and number of these phishing attacks have increased. In cases where the ATO has identified affected taxpayers, the ATO has contacted these people to inform them that they are a victim of a scam.

8. This year, as of the 1st of May, the ATO has received 4,002 reports from the public about phishing e-mails using the ATO brand. From these reports, the ATO has identified 67 unique URLs (web addresses) being used which is up from the 49 identified during the same time period last year.

9. To date, the ATO has not observed any cyber tax related scam or incident that specifically targets senior Australians.

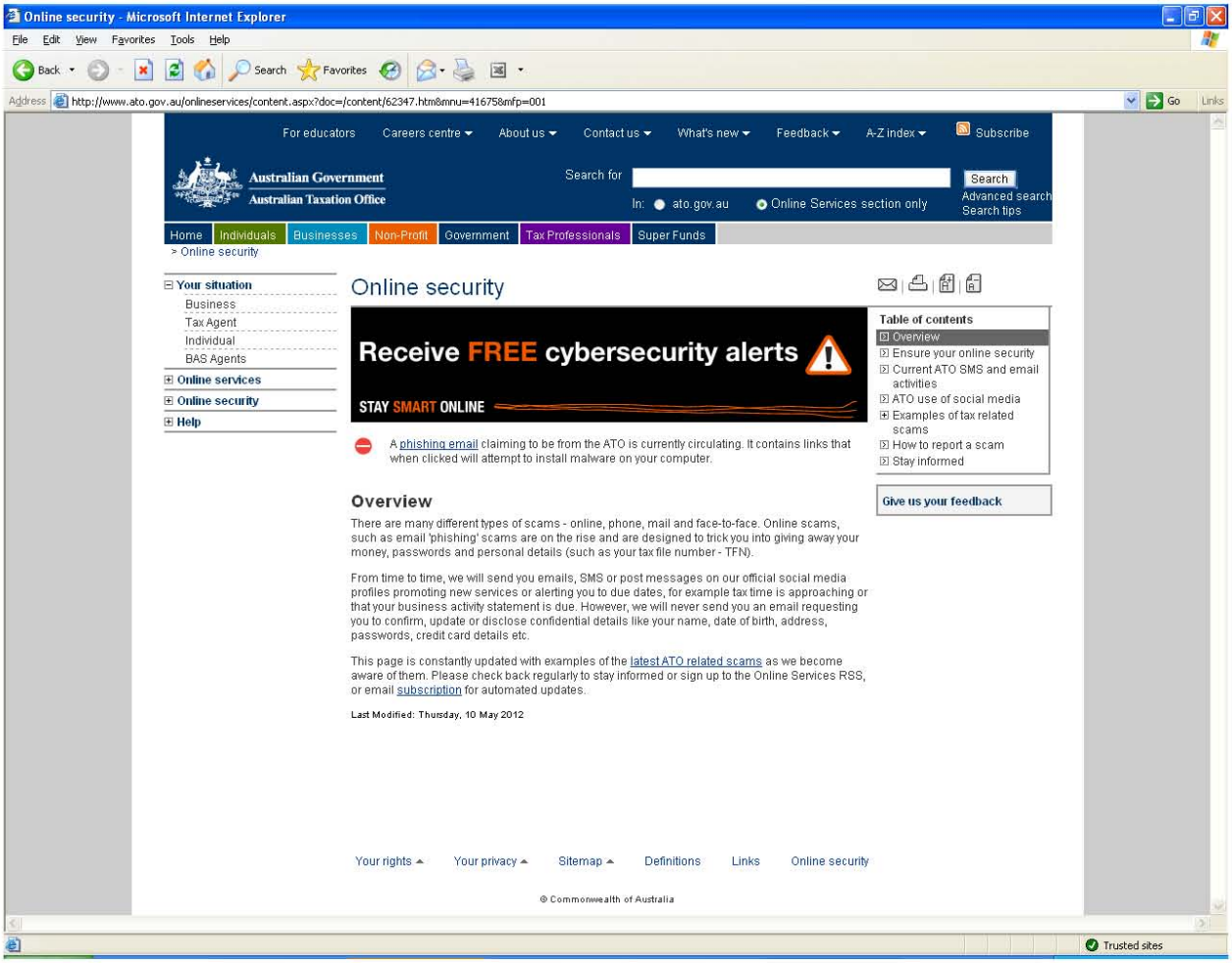
Current ATO Cyber security arrangements – IT Security Incident Response

10. The ATO provides a 24x7 IT Security Incident Response service with reporting, response and monitoring capability. This function revolves around having qualified staff who are on-call to manage and triage any event that could be an IT security incident. Additionally, development and implementation of the Security Analysis Toolkit (SAT), a customised application for managing and processing information and data, allows proactive identification of anomalous activity. Through the use of SAT, the Incident Response team have been able to identify further links to bogus websites (in association with the Tax Office Refund scheme) purporting to be the ATO, as well as other similar potential threats.

11. The ATO's Vulnerability Management and Research (VMR) team requests AusCERT to initiate take-downs of scam sites that seek to enable cyber crime acts. AusCERT is the Computer Emergency Response Team (CERT) in Australia and a leading CERT in the Asia/Pacific region. They are part of the global CERT teams and through these relationships, are able to assist with website shutdowns. The VMR team also forensically analyse the sites to understand the technical methods utilised by scammers.

12. Additionally, the VMR team manages the "reportemailfraud" mail box for notifications from the public of scams and other potential technology enabled crimes, and investigates issues relating to IT security breaches. Furthermore, the "Online Security" page on the ATO website (shown in Figure 1 below) details other mechanisms including phone contacts and online reporting forms for issues around tax evasion – Tax Evasion Referral Centre (TERC) forms.

Figure 1. The ATO's Online Security webpage



13. When the ATO is investigating a scam and becomes aware of compromised taxpayer information, the IT Security Incident Response team liaises with the ATO Call Centres to contact and advise each member of the public who may have had their personally identifiable information stolen. This can include such details as name, address, phone, Tax File Number (TFN), bank accounts, driver's licence number.

14. Through the IT Security Incident process, the Incident Response team provides information, data and images for publication on the ATO website as scams are uncovered. This provides an expeditious process to inform the public of new and significant variants of scams. The recent scams are highlighted as a headline for a period of time to ensure easy and obvious dissemination of this event. This is part of a comprehensive array of Online Security information the ATO provides to the public on its website and includes a link to "Protecting your Computer against Malicious code" which is provided by AusCERT.

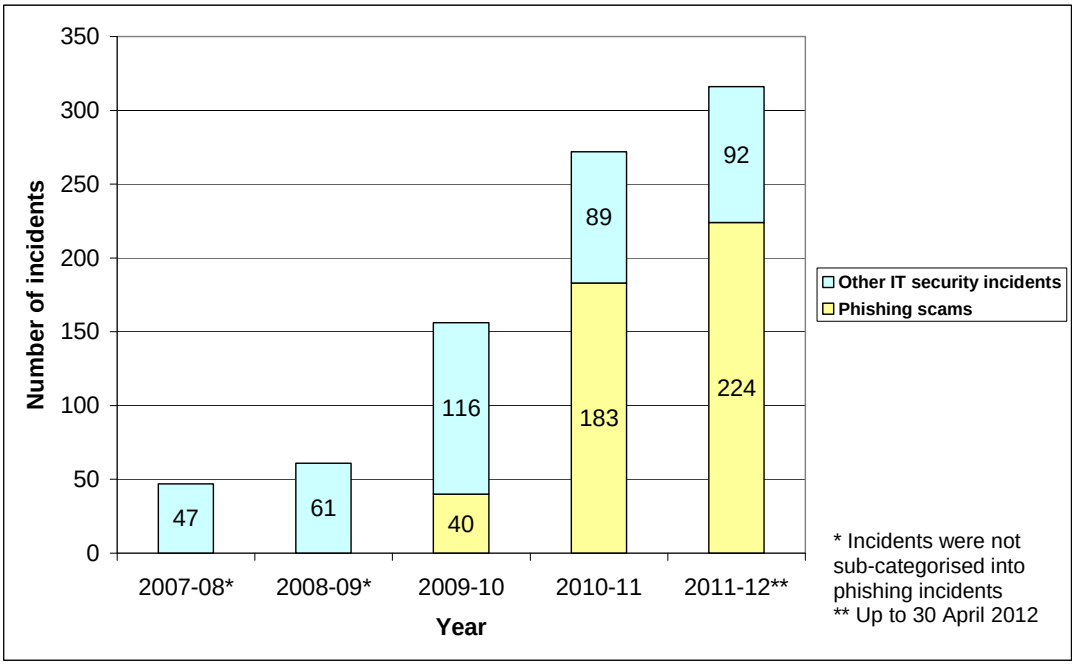
Trends

15. The most prevalent form of IT security incident is the online scam commonly known as the "Tax Office Refund" phishing scam. This scam attempts to entice people into handing over their personally identifiable information, usually by clicking a link in an email and completing the online form (for an example of this scam, please refer to Figure 4 below).

16. These phishing attacks are now more sophisticated and the ATO's observation is that:
    - The main purpose of these attacks is information gathering i.e. identity credentials, accounts and financial details etc.
    - Attacks are no longer about obtaining personal information once off but about gaining an ability to access systems and maintaining that access to perform identity theft and to gather information covertly.
    - There has been a 74.4% per cent increase in the total ATO IT security incidents for 2010-11 (over 2009-10) and the trend is expected to continue into the next year. Of the total IT security incidents in 2010-11, 67% were phishing incidents (see Figure 2 below)
    - From July 2011 to April 2012 inclusive, the ATO has experienced 306 IT security incidents and 71% of these were phishing incidents.
    - The increase in IT security incidents including the above observations are a consistent trend globally.

17. As mentioned above, there has been a growth in ATO IT security incidents, particularly relating to phishing scams as shown in Figure 2 below. An IT security incident refers to any action that result in harm or the significant threat of harm to ATO computer system/s or data.

Figure 2. Growth in ATO IT Security Incidents



18. The ATO has in-place a 'phishing-filter' which is used to disrupt scams utilising ATO resources. The 'phishing-filter' was used extensively against ATO branded phishing scams between 2007-2009, however the scammers have changed methods and the phishing-filter cannot be used to disrupt most recent attacks.

19. The ATO brand was used in several different fax related scams perpetrated in March 2012. The biggest of these scams involved faxes sent to real-estate agents advising of a 'rental income without deduction of Australian Tax' and to forward a form to all of their landlords. The form was to be completed and faxed back to a designated number by the landlord. This method utilised the Real Estate agent as a trusted source to elicit information from the landlord.

20. In February 2011 and September 2011, the ATO brand was used to propagate malware[1] via links to malicious websites and also as malicious software in an attachment in an e-mail. The malware would compromise the user's computer, enabling the criminals to monitor and log all activity performed on the computer.

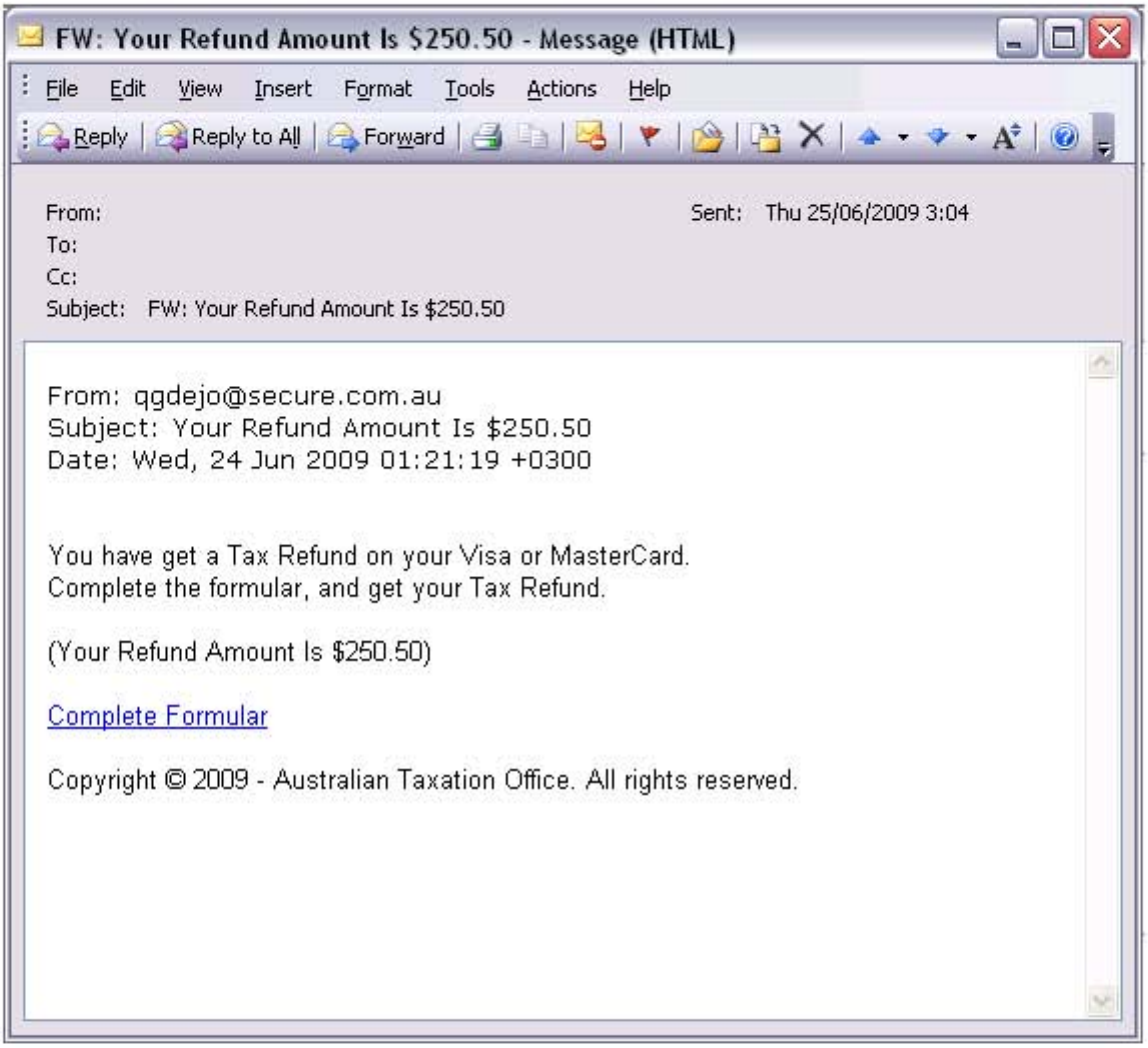
21. In September 2011, the Australian Business Register brand was used for the first time in a major phishing attack used to distribute malware. As above, the malware would compromise the user's computer, enabling the criminals to monitor and log all activity performed on that computer. Of course, if people have up-to-date anti-virus and anti-malware installed on their computer then it might help to reduce the risk.

22. Since Feb 2010, there has been a steady increase in phone scams. Some analysis of these scams indicate that the target audience is people who are not accessible online i.e. email. These scams are run in a similar manner to the online scams and are very cautious, structured and scripted. Logistically, they are harder to execute as it requires the scammers to acquire a contact number and a team of people to make/receive the calls in a Call Centre like construct. They utilise ATO details including titles, addresses and contact number/s and perform artificial Proof of Identity (POI) activities on the potential victim. In doing so they effectively elicit genuine personally identifiable information. Anecdotal evidence suggests that people falling victim to these scams are primarily retirees.

23. Evolution of phishing scams: The following screen-shots illustrate the increasing sophistication of phishing scams over time.

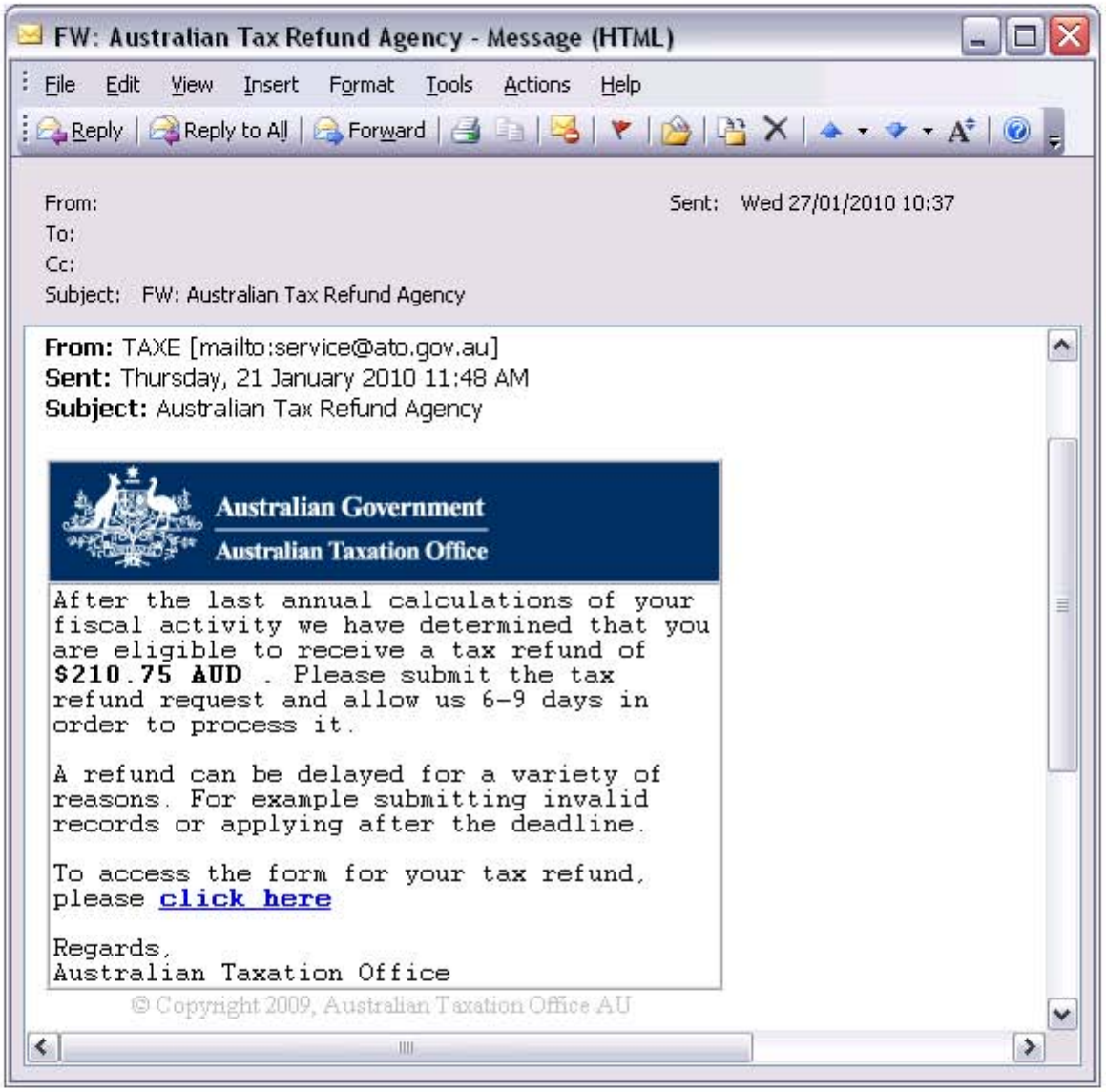
[1] Short for malicious software, malware is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.

Figure 3. Example of 2009 phishing email



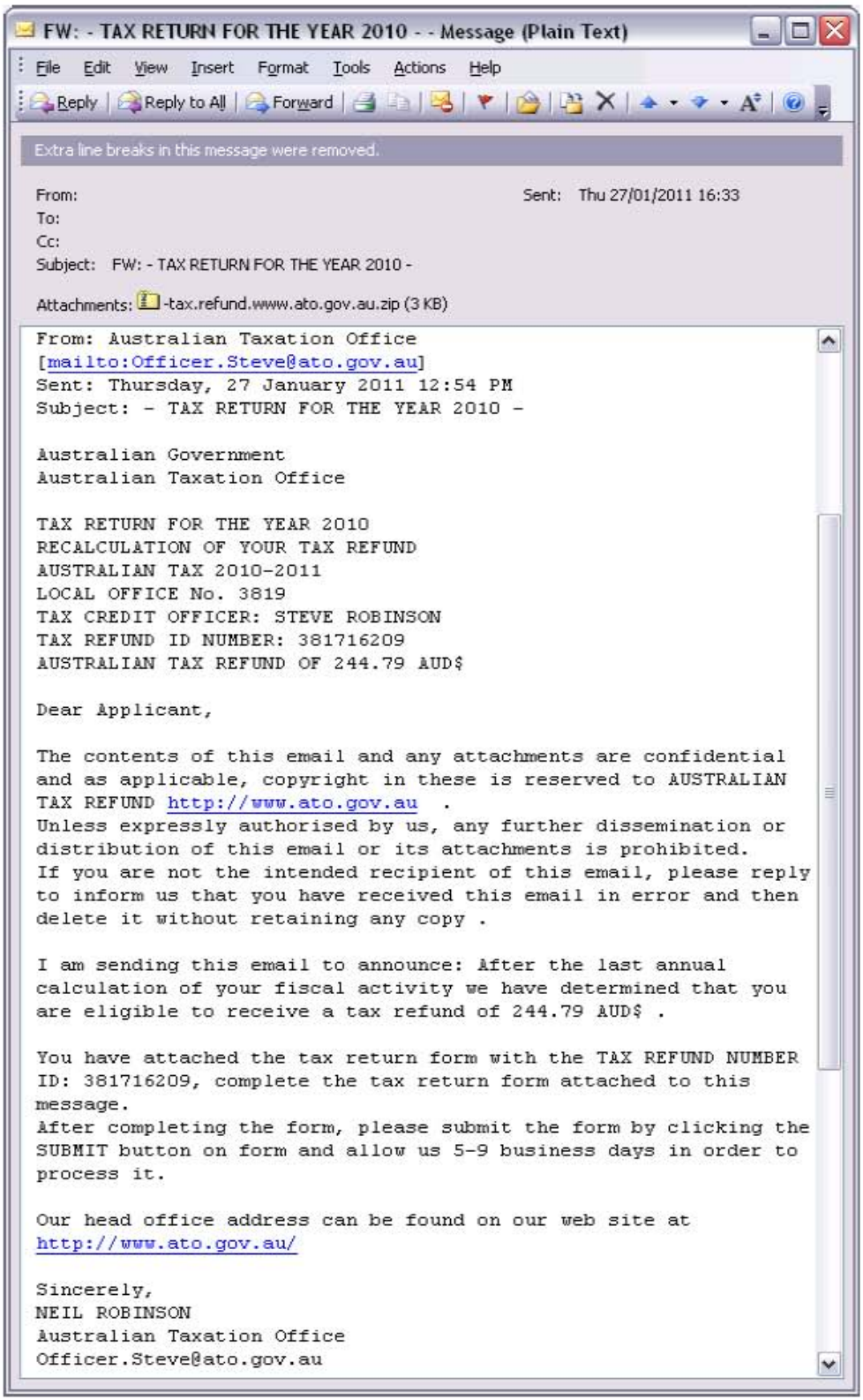
This e-mail is an example from a phishing attack experienced in 2009. The e-mail above was rather simplistic with a poorly worded paragraph and a link to a phishing website with limited use of the ATO brand.

Figure 4. Example of 2010 phishing email



This phishing e-mail was sent in 2010. This attack was more sophisticated and looked more legitimate than the previous one. This e-mail used the ATO logo to make the e-mail seem more legitimate. The e-mail address that sent the e-mail was also masquerading as an 'ato.gov.au' address.

Figure 5. Example of 2011 phishing email



FW: - TAX RETURN FOR THE YEAR 2010 - - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

Extra line breaks in this message were removed.

From: Sent: Thu 27/01/2011 16:33
To:
Cc:
Subject: FW: - TAX RETURN FOR THE YEAR 2010 -

Attachments: -tax.refund.www.ato.gov.au.zip (3 KB)

From: Australian Taxation Office
[mailto:Officer.Steve@ato.gov.au]
Sent: Thursday, 27 January 2011 12:54 PM
Subject: - TAX RETURN FOR THE YEAR 2010 -

Australian Government
Australian Taxation Office

TAX RETURN FOR THE YEAR 2010
RECALCULATION OF YOUR TAX REFUND
AUSTRALIAN TAX 2010-2011
LOCAL OFFICE No. 3819
TAX CREDIT OFFICER: STEVE ROBINSON
TAX REFUND ID NUMBER: 381716209
AUSTRALIAN TAX REFUND OF 244.79 AUD$

Dear Applicant,

The contents of this email and any attachments are confidential and as applicable, copyright in these is reserved to AUSTRALIAN TAX REFUND http://www.ato.gov.au .
Unless expressly authorised by us, any further dissemination or distribution of this email or its attachments is prohibited.
If you are not the intended recipient of this email, please reply to inform us that you have received this email in error and then delete it without retaining any copy .

I am sending this email to announce: After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of 244.79 AUD$.

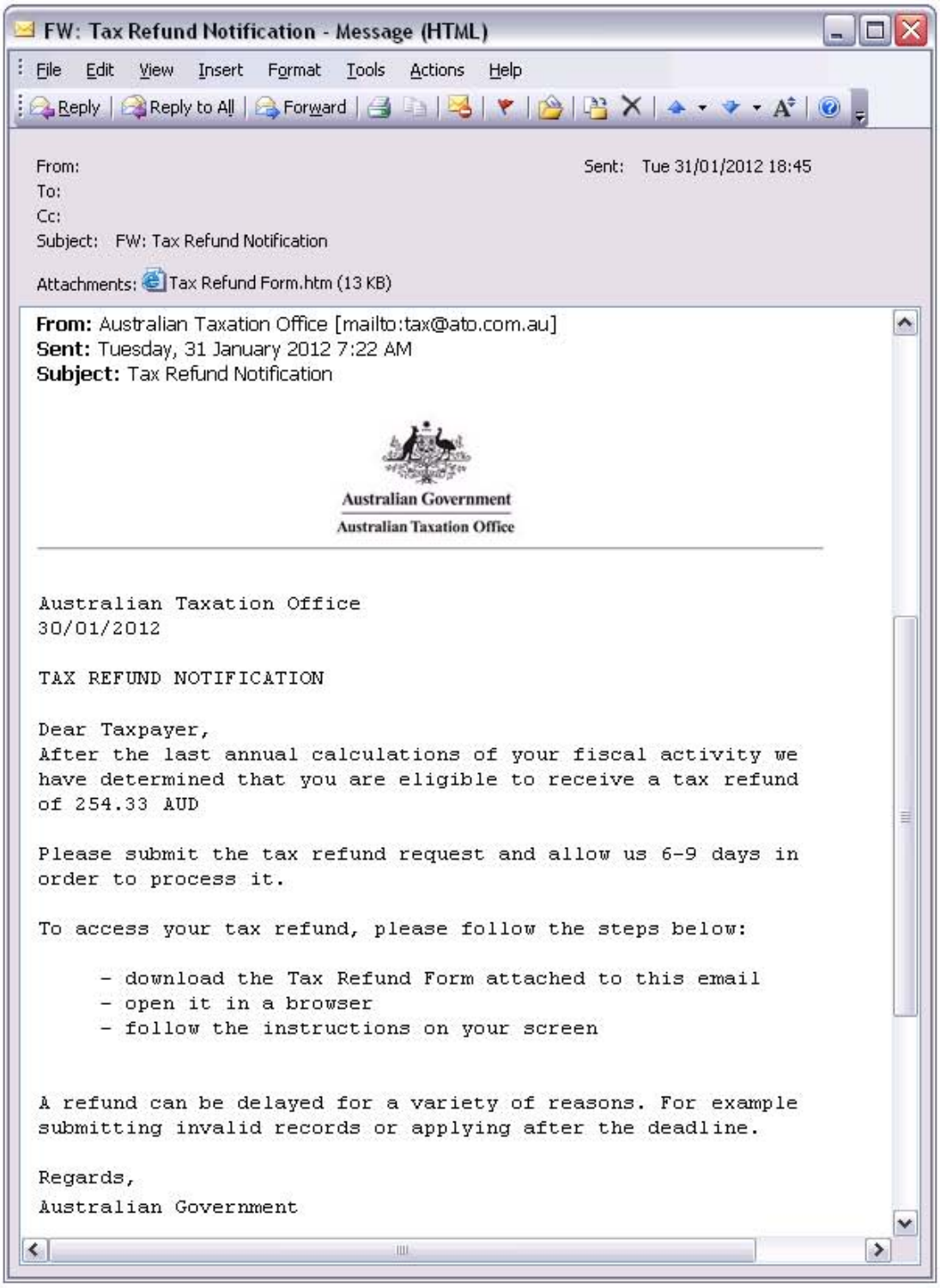
You have attached the tax return form with the TAX REFUND NUMBER ID: 381716209, complete the tax return form attached to this message.
After completing the form, please submit the form by clicking the SUBMIT button on form and allow us 5-9 business days in order to process it.

Our head office address can be found on our web site at http://www.ato.gov.au/

Sincerely,
NEIL ROBINSON
Australian Taxation Office
Officer.Steve@ato.gov.au

This e-mail was part of a phishing attack in 2011. This attack used a masquerading 'ato.gov.au' e-mail address. The attack also used fake ATO staff details in the signature block, e-mail address and body of the email.

Figure 6. Example of 2012 phishing email



FW: Tax Refund Notification - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: Sent: Tue 31/01/2012 18:45
To:
Cc:
Subject: FW: Tax Refund Notification

Attachments: Tax Refund Form.htm (13 KB)

From: Australian Taxation Office [mailto:tax@ato.com.au]
Sent: Tuesday, 31 January 2012 7:22 AM
Subject: Tax Refund Notification

Australian Government
Australian Taxation Office

Australian Taxation Office
30/01/2012

TAX REFUND NOTIFICATION

Dear Taxpayer,
After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of 254.33 AUD

Please submit the tax refund request and allow us 6-9 days in order to process it.

To access your tax refund, please follow the steps below:

- download the Tax Refund Form attached to this email
- open it in a browser
- follow the instructions on your screen

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

Regards,
Australian Government

This phishing e-mail was sent in 2012. This attack used an official looking e-mail with directions to open an attachment. The attachment redirected users to an ATO branded phishing website. This e-mail was set-out more clearly then previous e-mails with clear instructions.

Community Communication and Awareness

24. The ATO employs an extensive awareness strategy to help inform the community on what they can do to interact safely with the ATO via:
    - Media releases
    - The ATO website (www.ato.gov.au)
    - TV interviews
    - Seminars
    - Multilingual media e.g. SBS radio
    - Slam Scam! Awareness Week
    - YouTube media publications
    - Publications to the Tax Practitioners group.

25. The ATO publishes extensive information on scams currently being perpetrated. Such information can be obtained from the ATO website at the "Online security" link on the home page (shown above in Figure 1). Examples of the current scams and previous scams are presented along with any particular issues or concerns.

26. Between January and December 2011, the ATO issued four scam-related media releases that were translated in six languages and distributed to over fifty ethnic media outlets.

27. AusCERT publishes alerts on our behalf to the staysmartonline.gov.au website. Several warnings in relation to ATO branded phishing emails have been published by AusCERT including a Staying Smart Online alert on the use of a new template (9 June 2011).

28. During July to October 2011, messages warning of tax related scams targeting diverse audiences were included in SBS in-language radio announcements, in-language seminars and articles in non-English speaking background intermediaries' newsletters.

Other Issues and Recommendations

29. The ATO is working with the Australian Communications and Media Authority (ACMA). When the ACMA Spam Intelligence Database (SID) identifies fraudulent ATO related e-mails, an automated report is sent to the ATO for further analysis and action.

30. The ATO is an active member of the Australasian Consumer Fraud Taskforce (ACFT). The ATO regularly contributes to the ACFT and their related initiatives such as the National Consumer Fraud Week.

31. Analysis by the ATO Incident Response team of the personal information of people who have fallen victim to a scam (i.e. Australian citizens who have given their personally identifiable information to the scammers) indicates that senior Australians constitute a minority. While this is true in the current environment, expectation is that with further delivery of services through the online environment, this could well increase.

32. The ATO has recently formed a partnership with the Rev-Sec Group. The Group is a community of revenue collection agencies – HMRC, NZ IRD, US IRS, Canada CRA, and the ATO, with the focus on reputational abuse in the conduct of scams and financial fraud schemes.

33. The seniors segment of the population, which is a growing demographic in our community, is clearly exposed to the risks around the use of information technology. Acknowledging this growth and the greater take up by senior Australians of online services, the ATO believes that there is an increasing chance of loss or compromise of personally identifiable information in the future. There is a need to ensure that they apply good online security practices and procedures. The delivery of education and awareness to senior Australians either through sessions at community colleges or other community like services would help improve the level of knowledge and understanding in this area.

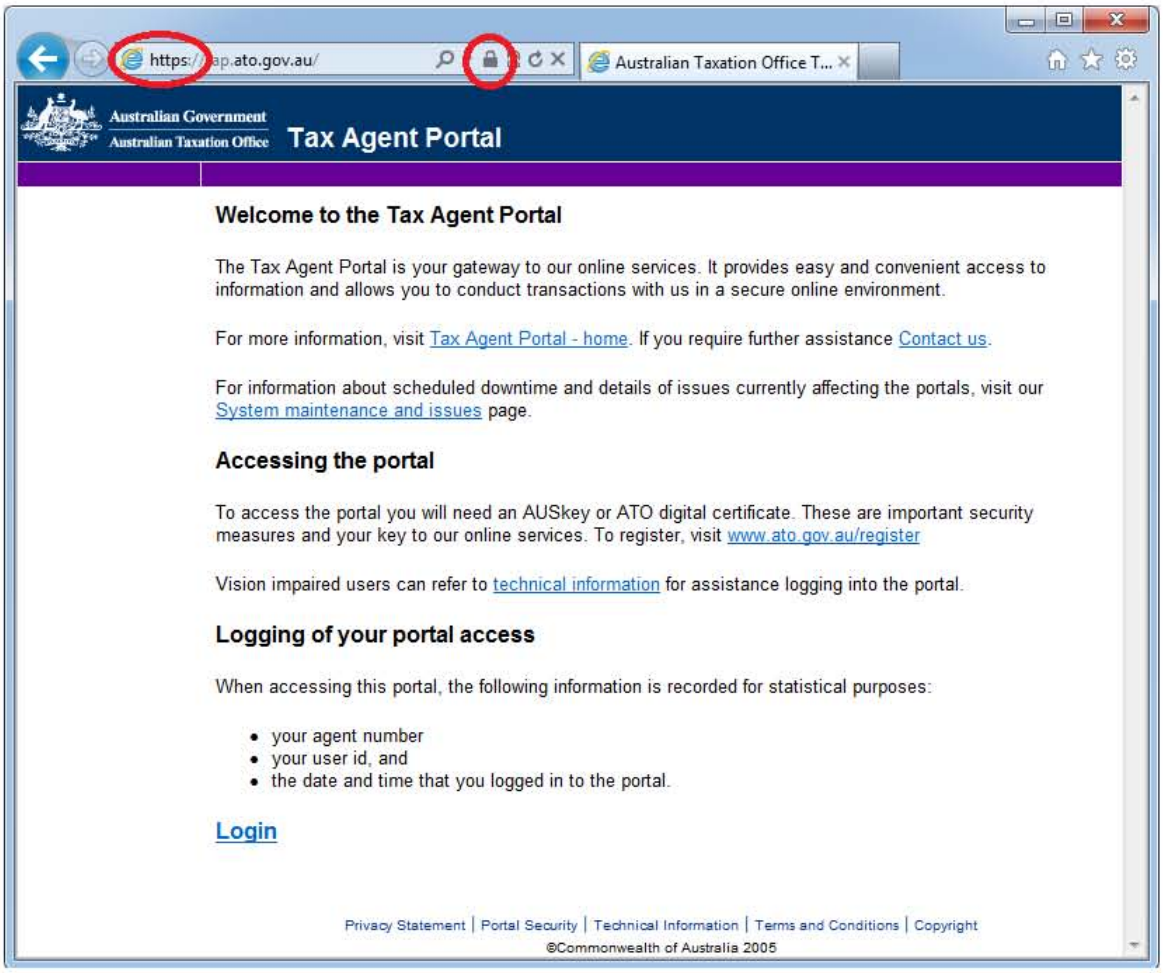
34. There is no doubt that as more enterprises interact with clients online, this will contribute to the advent of new and innovative scams. All agencies and corporations should be encouraged to participate in creating a culture of online security awareness. They can start by providing easily accessible information of good online security practices on their websites.

35. The ATO has implemented technologies which allow a greater level of confidence around the authenticity of an email[2]. Adoption of such technology by organisations enables the receiving client or client software to verify to a higher level of assurance that an email has come from a legitimate sender.

36. Similarly, users should be aware that when communicating sensitive information such as personally identifiable information and financial information, the information should be sent to the website in an encrypted manner. They can do this by ensuring that their browser displays an “https” and/or “padlock” icon as shown in Figure 7 below.

[2] These include the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM).

Figure 7. Example of “https” and “padlock” icons



37. Users should always verify the site that they are on is ‘ato.gov.au’. This can be done by checking the URL in the browser or by typing in the web address into the browser, rather than clicking on a link embedded in an email.

Prepared: 15 May 2012.