

Case study: personalised phishing site

Summary	1
Details of the attack	2
Initial email	2
Initial fraudulent site log in.....	3
Address verification	4
Authentication details	5
Final confirmation and redirect.....	6
Assessment.....	7
Prevention	7

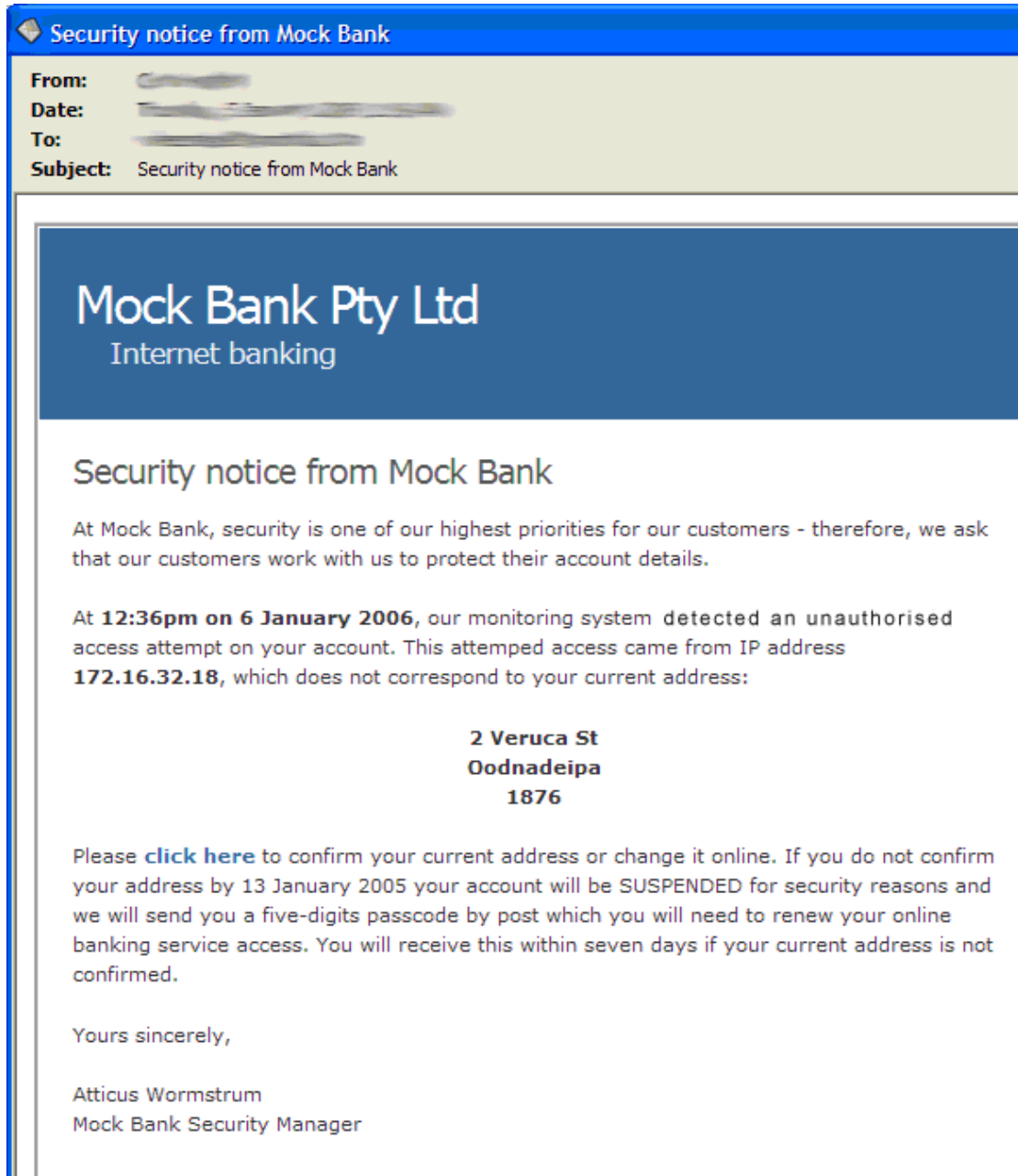
Summary

A phishing attack has been seen recently in the wild where the attacker strengthened the credibility of their fraudulent site by including legitimate, previously obtained user details, such as home addresses and card numbers. The site displays information tailored for each user.

Details of the attack

A financial institution was targeted in this attack – a re-creation is provided below. Bank customers received the email below:

Initial email



The address listed corresponded to each recipient's current address or a past address. The 'click here' link contained a link to a fraudulent web site with a tracking code to identify each customer.

Initial fraudulent site log in



Upon clicking the link within the email, the potential victim (user) will see the Initial login page (above).

The URL in the address bar at the top of the browser contains two items of note:

- The domain name, `online.mockbank.com.au.example.com`, shows that the attacker controls `example.com`, and has constructed a sub-domain to attempt to confuse bank customers.
- The `'userid=ab94e1'` contains a unique identifier used by the attacker to determine which potential victim is visiting the fraudulent site, and to tailor the fraudulent website display accordingly.

Address verification

The screenshot shows a Mozilla Firefox browser window with the title 'Mock Bank Pty Ltd: Internet Banking'. The address bar displays the URL 'http://online.mockbank.com.au.example.com/login.html?userid=ab94e1'. The page content includes a header for 'Mock Bank Pty Ltd Internet banking' and a navigation bar with four tabs: 'LOG ON', 'ADDRESS VERIFICATION' (which is highlighted), 'SECURITY CHECK', and 'CONFIRMATION'. Below the navigation bar, the 'Address verification' section contains the text: 'We currently have the following details on file for you. If these are incorrect, please update them:'. This is followed by three input fields: 'Current address:' with the value '2 Veruca St', 'Oodnadeipa', and 'Postcode:' with the value '1876'. At the bottom of the form area, there are two links: '< Prev' and 'Next >'. A footer at the very bottom of the page reads '© Mock Bank Pty Ltd, 2006'.

If the user enters their last name and card number and proceeds to the next step, they are presented with an address verification step, filled with the same pre-populated data provided in the initial email. The address displayed is personalised for each user, and likely drawn from a text or relational database matched against their unique identifier.

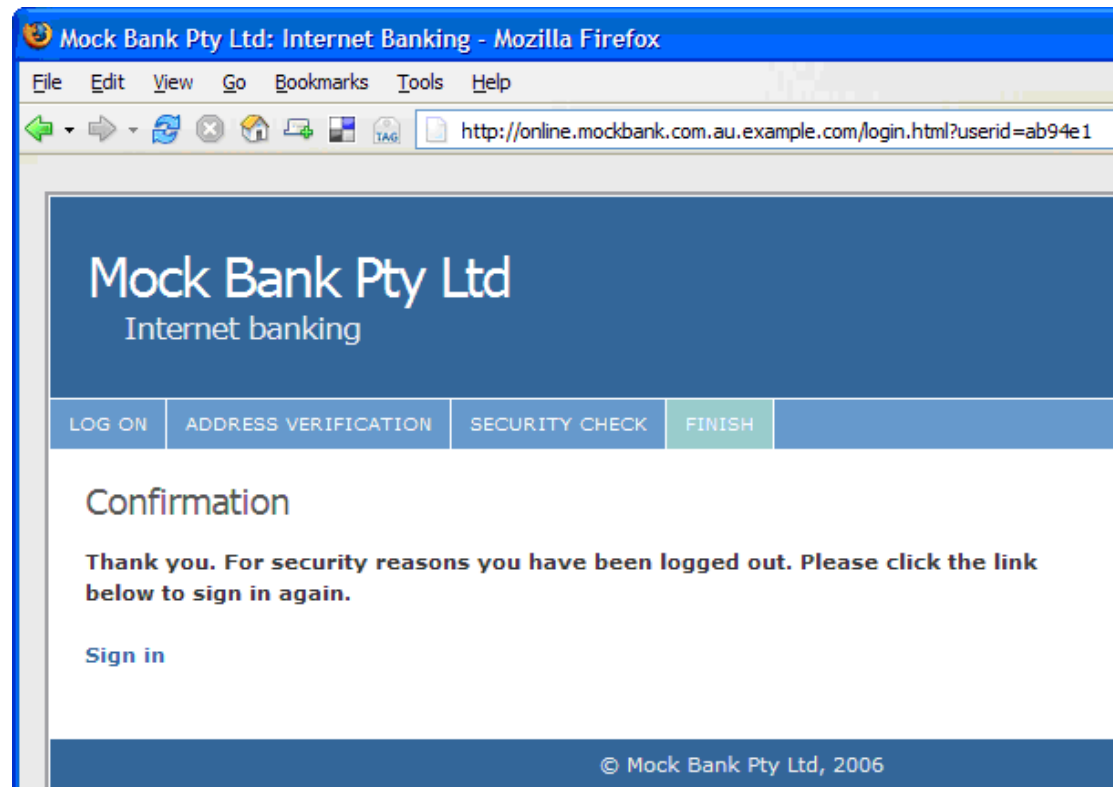
This approach increases the level of credibility of the scam and additionally allows the attacker to gain the victim's updated personal details.

Authentication details

The screenshot shows a web browser window titled "Mock Bank Pty Ltd: Internet Banking - Mozilla Firefox". The address bar displays the URL "http://online.mockbank.com.au.example.com/login.html?userid=ab94e1". The page header features the "Mock Bank Pty Ltd Internet banking" logo. Below the header is a navigation bar with five tabs: "LOG ON", "ADDRESS VERIFICATION", "SECURITY CHECK" (which is highlighted in green), "CONFIRMATION", and an empty tab. The main content area is titled "Security check" and contains the text: "Before we can finalise your changes, we need to verify your security information:". Below this text are two input fields: "Password:" and "Answer to secret question:". At the bottom of the form area are two buttons: "< Prev" and "Finish". The footer of the page displays the copyright notice "© Mock Bank Pty Ltd, 2006".

Once the user has confirmed or updated their address details, they are prompted for their password and other authenticating details. Presumably, the attacker hopes that displaying knowledge of data known to the user will increase the likelihood of them providing authentication data in the final stage.

Final confirmation and redirect



The 'Sign in' link now redirects the victim to the real bank site at <http://online.mockbank.com.au/login.html>. This increases the chance that the victim will be unaware that they have provided their details to the attacker, and will maximize the time the attacker has to clear the funds from the victim's account.

Assessment

The details used by the attackers in this case were likely obtained from another source, such as breach of a commercial website or resold customer database. The fraudulent site likely employs sophisticated custom coding as well as a back end repository of customer data to serve and store captured details.

This once again highlights the increasing sophistication of identity theft attacks against members of the public.

Prevention

- Never click on links in emails, especially if they purport to come from a financial institution, no matter how credible they may appear.
- Verify receipt of such an email with the named institution to determine if it is genuine.
- Check that the page is running over a secured connection, via an <https://> address in the address bar and the web browser's 'golden padlock'.
- No warnings should be displayed by the browser when validating a certificate from a web server. A valid certificate should:
 - have a Common Name exactly matching the site address visited;
 - not be expired;
 - have a trusted certificate issuer. This is particularly important since it is trivial for an attacker to self-sign a certificate with valid Common Name and expiry data.
- In this case, the attack used the domain `online.mockbank.com.au.example.com`. Carefully check the domain name of any URL to determine that it is an exact match for a trusted institution's.