



Factsheet 9 – What is a web site digital certificate and why is it important to check?

Web site digital certificates can help users decide when it is safe to transact online and when it is not; and when it is safe to use a web site that allows you to store or access personal or business information about yourself or your business.

This factsheet explains:

- When it is appropriate for a web site to provide a digital certificate and when it is not necessary,
- how to check if a digital certificate is present on a web site,
- if present, how to check if the certificate is valid; and
- whether it should be trusted.

Users that have a better understanding of how SSL and digital certificates contribute to online security and trust will be better able to:

- detect fake (phishing¹) web sites which are set up by criminals to capture users' online account passwords and other sensitive information;
- detect when a web site is transmitting users' personal and sensitive information over the Internet in an unencrypted format; and
- protect themselves from online fraud.

What is a web site digital certificate?

A digital certificate is a mechanism for users to obtain assurance about the identity and authenticity of a web site. By inspecting the digital certificate on a web site, users can help prevent identity theft and fraud. For example, a phishing site set up by

¹ To understand more about phishing attacks, see http://www.staysmartonline.gov.au/factsheets/factsheet_10



criminals which masquerades as a legitimate web site (such as an online banking web site) can often be identified by an invalid or absent digital certificate.

Digital certificates are implemented as part of a set of security mechanisms provided by SSL.² SSL encrypts³ all traffic sent between a user's computer and a remote web site to prevent the data being read in transit as it passes from a user's computer (the client computer), across the Internet to the web site (server computer) and back again.

When is it appropriate for a web site to provide a digital certificate?

Generally, any web site that requires you to provide a user name and password, or allows you to submit or provides access to your personal or business financial information should provide an SSL connection to the web site, which is evident by the presence of 'https' in the browser address bar.

The absence of a digital certificate means that the content sent or received to and from the web site is not encrypted, and can potentially be seen by other parties. The risk of this information being seen by others is particularly high if this *information is being accessed or submitted while using an unsecured (unencrypted) WiFi access point.*

- If you wish to connect to a web site that holds your sensitive information then you should immediately check for the presence of a valid digital certificate.
- Whenever you connect to an SSL enabled web site, it will provide a digital certificate, although it is not always readily visible.⁴
- As a general rule, **do not** provide login credentials or other personal information to any web site that does not correctly implement SSL digital certificates.

² SSL stands for Secure Sockets Layer; it is analogous to TLS (Transport Layer Security).

³ Encryption is the process by which information is encoded using a special key to make it meaningless to anyone who has access to the encrypted data when it is sent over the Internet. Only the user or the computer with the key can decrypt the data to make sense of it.

⁴ Problems arise when accessing an SSL protected web site from a mobile device such as a phone. Browsers on handheld devices such as mobile telephones do not provide the same visual clues and make it more difficult to check the security of the Internet connection, which is critical if using an unsecured WiFi network. The advice in this factsheet relates only to computer browser access from a laptop computer or ordinary workstation, PC or Mac, not from hand held mobile devices.



Different web browsers display digital certificate information in slightly different ways

The following examples show how the Mozilla Firefox and Microsoft Internet Explorer web browsers display digital certificates.

Mozilla Firefox

Figure 1 shows the logon page for the Australian government Centrelink web site using the Mozilla Firefox web browser. Web sites which implement SSL have the following features:

- Use 'https://' in the browser address bar (as circled in figure 1) indicating that the connection is encrypted
- a padlock, which contains the information about the digital certificate. If using Mozilla Firefox, the padlock appears in the bottom right corner of the browser.

Note that the Centrelink web site presents an SSL connection (as shown by the presence of the https) from the logon page, before the user submits any personal information, including a user's password to the web site.

This is the best approach as it allows the user to verify that their username and password will be encrypted before the user actually provides their customer access number and password.

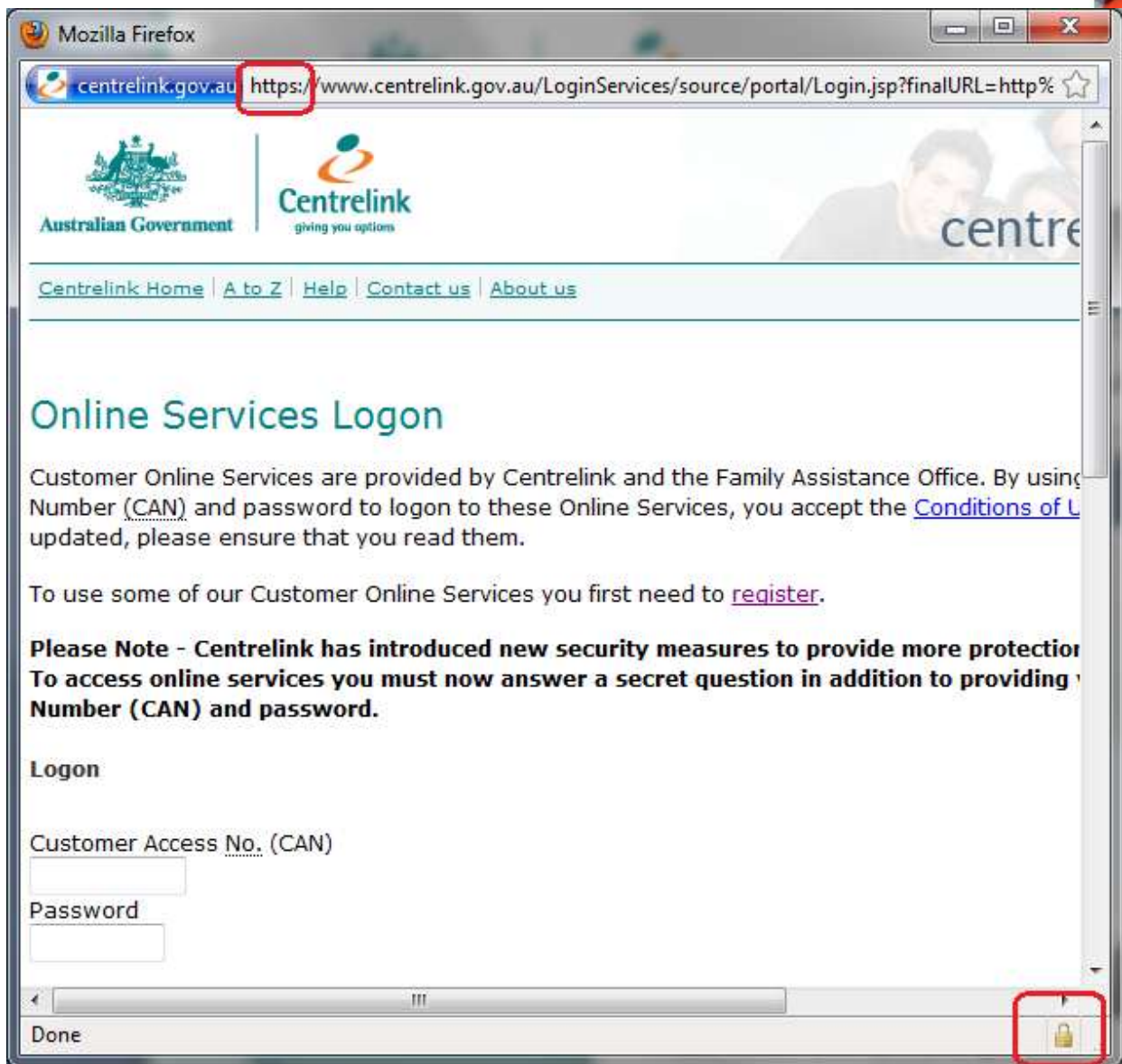


Figure 1, Mozilla Firefox, SSL session

You should always inspect the digital certificate of a web site if you intend to submit financial or personal identifying information (PII) to it.

To view more information about the digital certificate, double-click the padlock in the browser window.

Figure 2 is the page information which will be displayed by clicking on the padlock image.

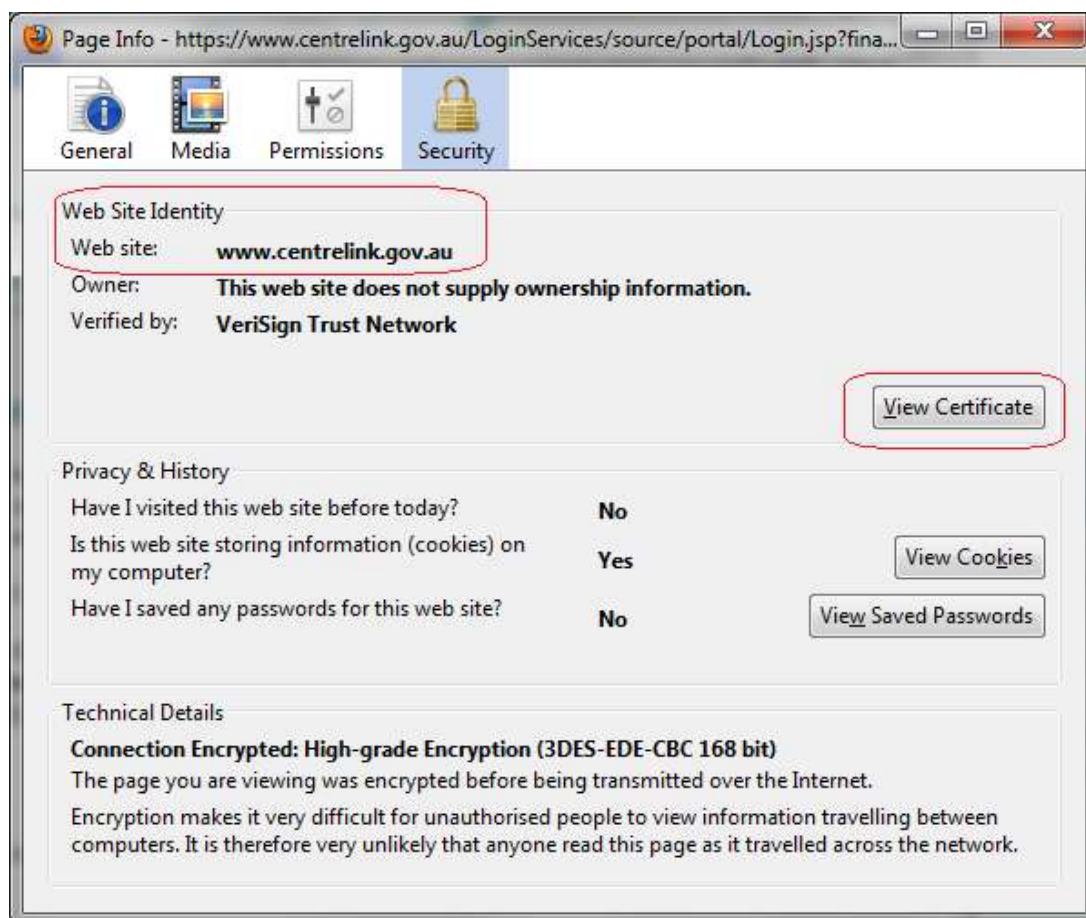


Figure 2, page information relating to the Centrelink digital certificate using the Mozilla Firefox browser

Figure 3 is the digital certificate, which will be displayed by clicking on the “View Certificate” button, shown in figure 2.

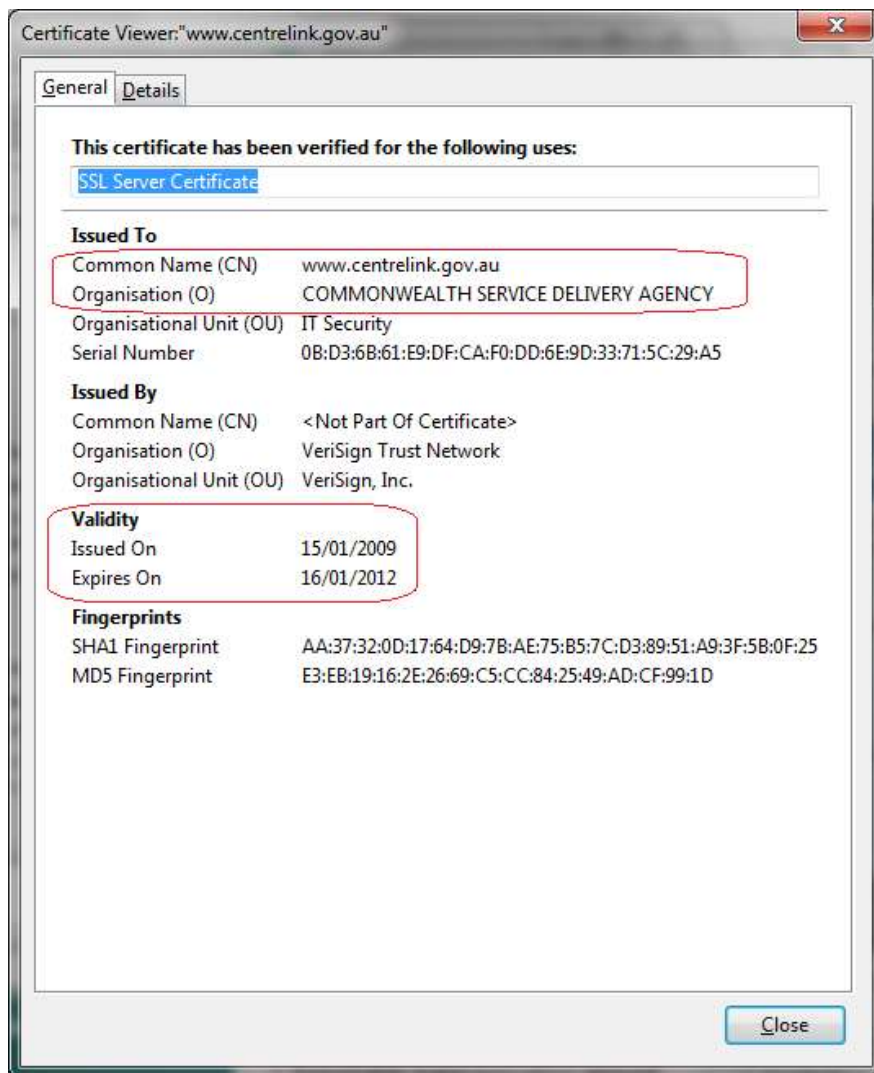
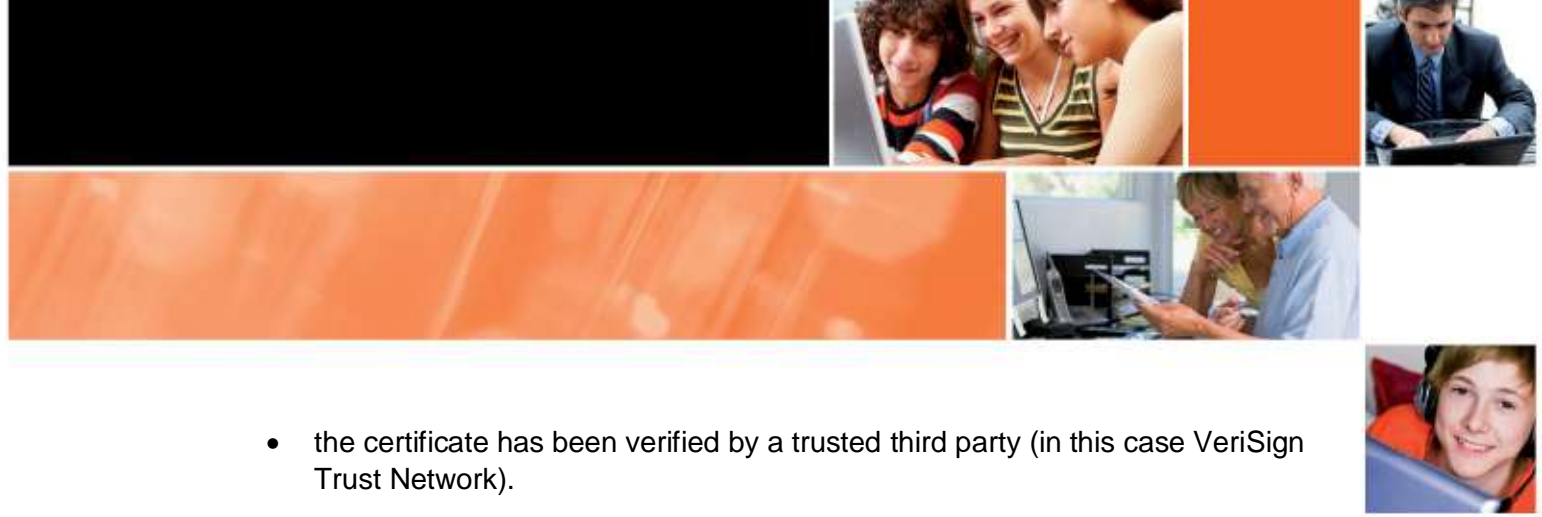


Figure 3, the Centrelink digital certificate as displayed in Firefox browser

The certificate states that a certificate authority (a trusted third party, called Verisign Trust Network) has verified the identity of the domain name www.centrelink.gov.au and that the certificate (at the time it was accessed) has not expired.

Therefore, we know this is a valid digital certificate which can be trusted because:

- it uses https in the browser address bar (see figure 1)
- the domain in the address bar www.centrelink.gov.au matches the domain contained in the digital certificate (compare figure 1 and 3)

- 
- the certificate has been verified by a trusted third party (in this case VeriSign Trust Network).
 - The certificate date has not expired (at the time this information was accessed).

Microsoft Internet Explorer

Figure 4 shows the logon page for the Australian government Centrelink web site using the Microsoft Internet Explorer web browser. Web sites which implement SSL have the following features:

- Use 'https://' in the browser address bar (as circled) indicating that the connection is encrypted
- a padlock, which contains the information about the digital certificate. The padlock appears on the right side of the browser address bar for Microsoft Internet Explorer.

Note that the Centrelink web site presents an SSL connection (as shown by the presence of the https) from the logon page, *before* the user submits any personal information, including a user's password to the web site.

This is the best approach as it allows the user to *verify* that their username and password will be encrypted *before* the user actually provides their customer access number and password.



https://www.centrelink.gov.au/LoginServices/source/portal/Login.jsp?finalURL=http%3A%2F%2Fmyacc - Windows ...

https://www.centrelink.gov.au/LoginServices/source/portal/Login.jsp?finalURL=http%3A%2F%2Fmyaccount.centrelink.gov.au

Australian Government | Centrelink giving you options

Centrelink Home | A to Z | Help | Contact us | About us

Online Services Logon

Customer Online Services are provided by Centrelink and the Family Assistance Office. By using your Customer Access Number (CAN) and password to logon to these Online Services, you accept the [Conditions of Use](#). These may have updated, please ensure that you read them.

To use some of our Customer Online Services you first need to [register](#).

Please Note - Centrelink has introduced new security measures to provide more protection for your online access. To access online services you must now answer a secret question in addition to providing your Customer Access Number (CAN) and password.


Logon

Customer Access No. (CAN)

Password

Done | Internet | Protected Mode: Off | 100%

Figure 4, Microsoft Internet Explorer, SSL session



You should always inspect the digital certificate of a web site if you intend to submit financial or personal identifying information (PII) to it.

To view more information about the digital certificate, double-click the padlock in the browser window.

Figure 5 is the security report which will be displayed by clicking on the padlock image.

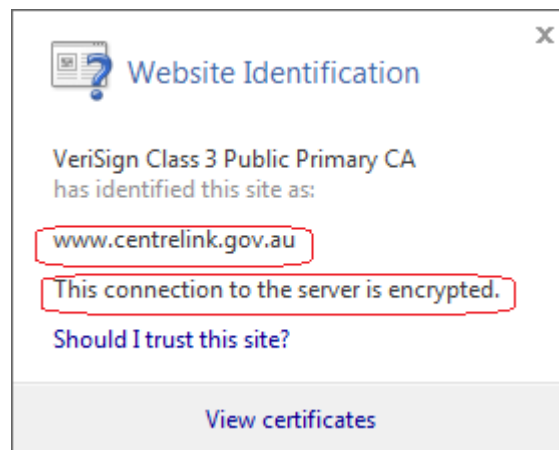


Figure 5, the security report for the Centrelink digital certificate using Microsoft Internet Explorer

Figure 6 is the digital certificate, which will be displayed by clicking on the “View Certificate” link, shown in figure 5.

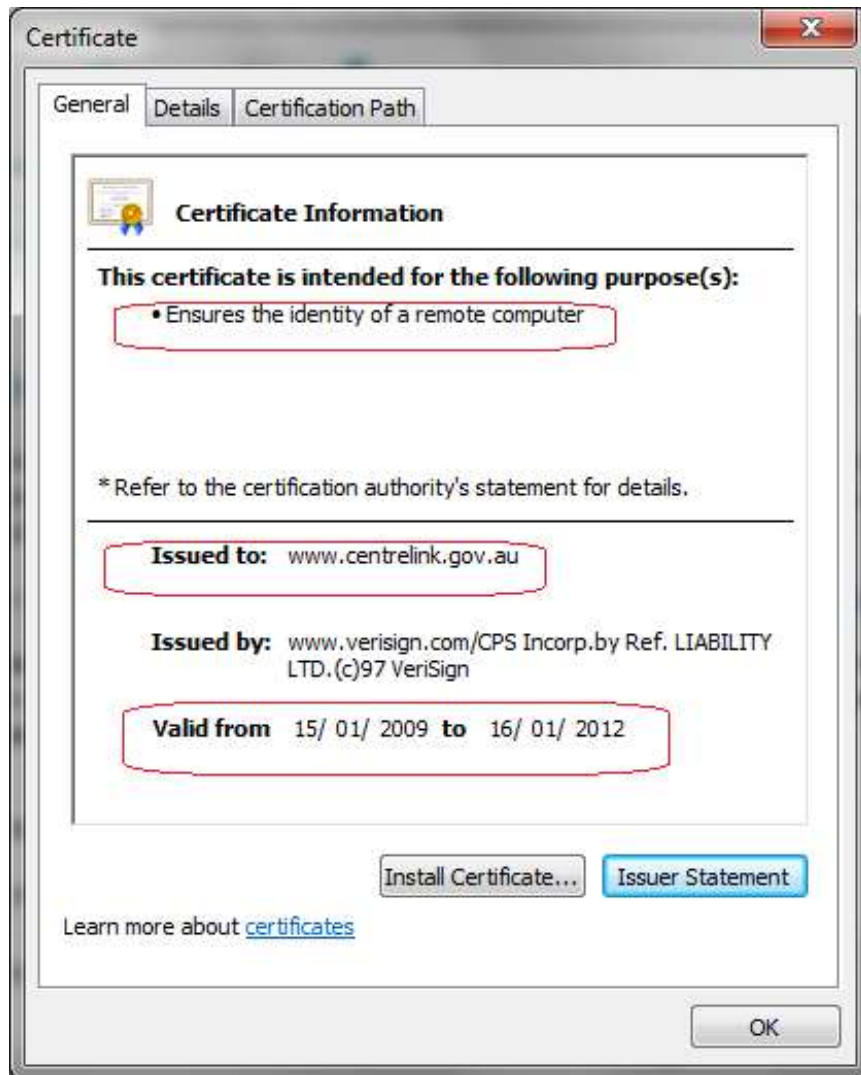
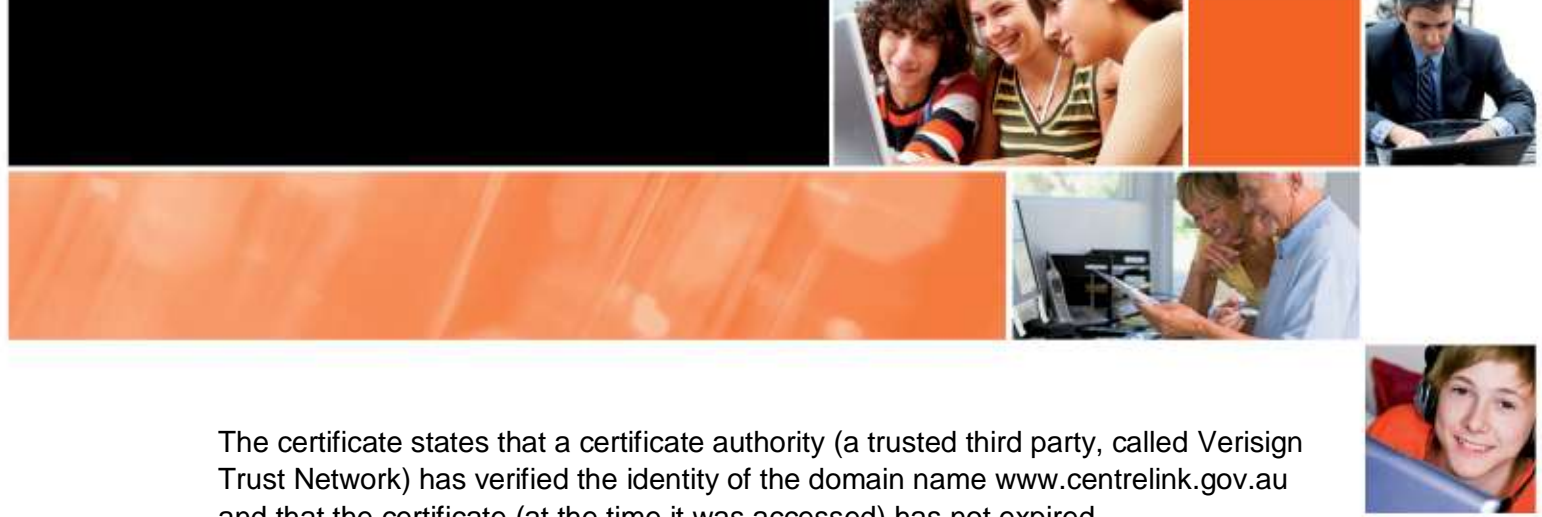


Figure 6, the Centrelink digital certificate as displayed with Microsoft Internet Explorer



The certificate states that a certificate authority (a trusted third party, called Verisign Trust Network) has verified the identity of the domain name www.centrelink.gov.au and that the certificate (at the time it was accessed) has not expired.

Therefore, we know this is a valid digital certificate that can be trusted because:

- it uses https in the browser address bar (see figure 4)
- the domain in the address bar www.centrelink.gov.au matches the domain contained in the digital certificate (compare figure 4 and 6)
- the certificate has been verified by a trusted third party (in this case VeriSign Trust Network)
- The certificate date has not expired (at the time this information was accessed).

Why should I inspect the digital certificate?

The web browser window is vulnerable to manipulation by criminals and the presence of a padlock image may not be enough to provide assurance of security, and by extension, trust. This means that once you have checked for the presence of the padlock, it is still wise to view and check the validity of the certificate itself.

When is checking for the presence of a valid digital certificate most critical?

Look for a valid digital certificate, when :

- The web site provides a logon page and/or
- collects or provides access to your personal or sensitive business information.

If there is no digital certificate in these situations then it is safer not to use or trust the web site.



In particular, the risks of failing to check for the presence of an SSL connection when accessing private or sensitive personal or business information is very high when using an unsecured (unencrypted) WiFi connection to the Internet.

So for example (as shown in figure 7 below), the Facebook web site provides a logon page but there is no digital certificate present. Hence prior to submitting the username and password, the user has no way to be sure that that the password will be encrypted when submitted; or that the web site belongs to the claimed entity.

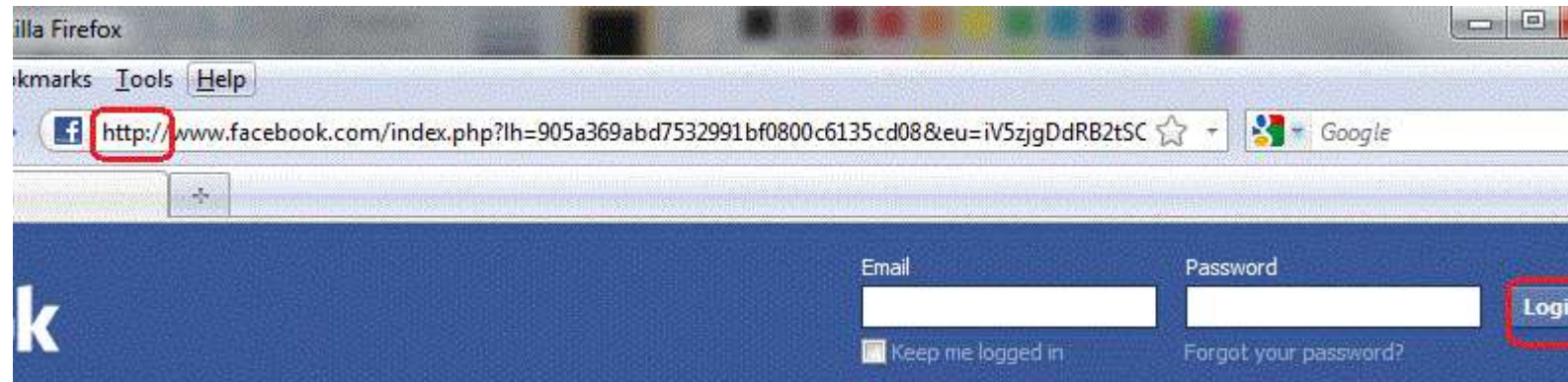
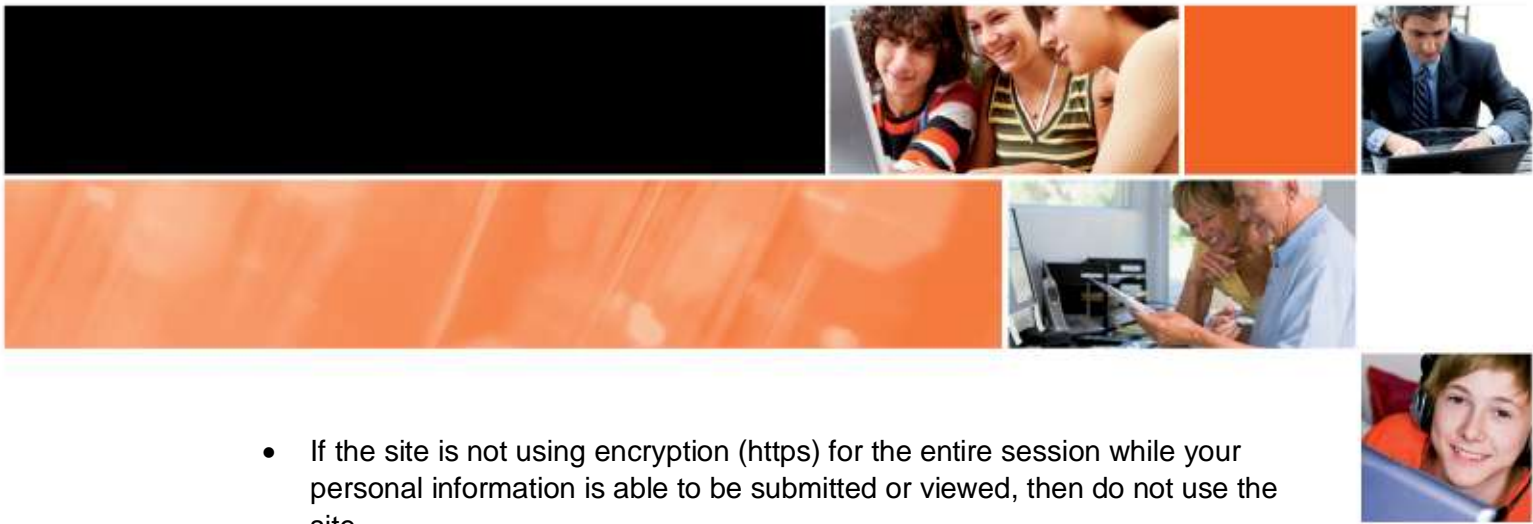


Figure 7, Mozilla browser HTTP log in page

There are tools available which make it trivial for people using the same unencrypted (unsecured) WiFi connection to easily intercept and view any of your traffic that is using only HTTP.

- If you cannot inspect the digital certificate of a web site to your satisfaction you should not submit information to the site. A disadvantage of using your mobile telephone to connect to secured sites is that the small interface generally does not allow the content of the certificate to be viewed and verified.



- If the site is not using encryption (https) for the entire session while your personal information is able to be submitted or viewed, then do not use the site.

Browser warnings

A browser will *not* warn you when a digital certificate should be present but is not. It is up to you, the user, to check to make sure the web site is using HTTPS *if you think it is appropriate to protect the confidentiality of the information being submitted or accessed via the web site.*

A web browser will warn users about problems with a digital certificate when:

- the certificate is self-signed or self-issued (this means no independent third party has verified that the domain belongs to the entity using it); or
- the domain name on the certificate does not match the domain name of the web site address in the browser.

Either of these warnings may indicate that the web site is not legitimate and has been created to fool users into disclosing sensitive or other personal information.

A web browser will warn users about problems with a digital certificate when:

- the site may be transmitting some parts of the page without encryption

This is potentially a serious problem if some of the content includes sensitive personal or financial information, especially if you are accessing the web site from an unsecured public WiFi hotspot. Figure 8 below provides an example of this browser warning after logging into the Facebook web site.

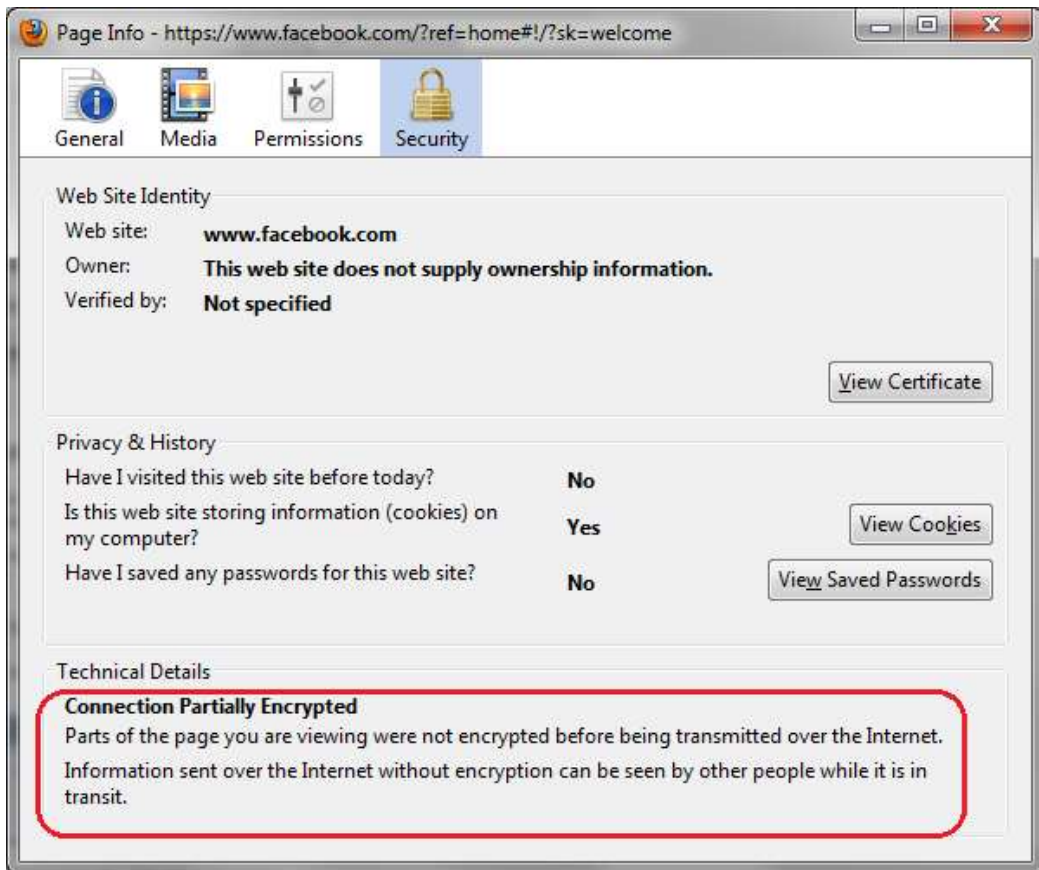


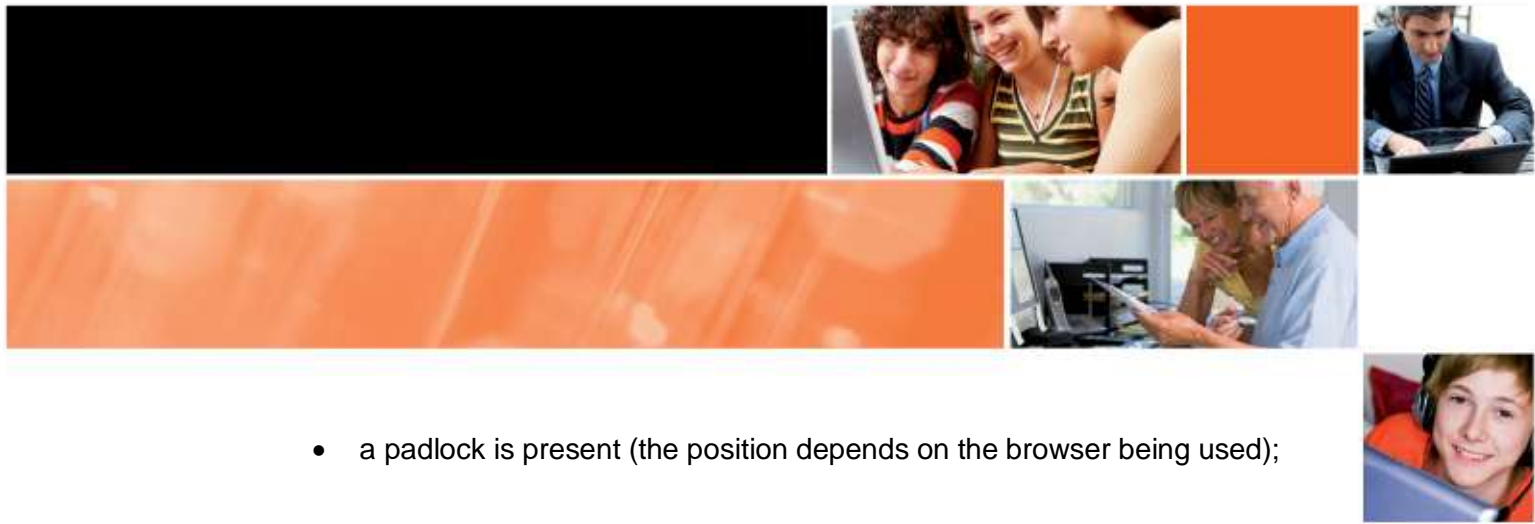
Figure 8, information warning that some content is not encrypted on the above page.

In this situation it is safer to avoid connecting to the web site until you can do so from a more secure location, such as a home or work network that does not use an unsecured (unencrypted) WiFi network.

How do I check if the digital certificate is valid?

In all cases, browser warnings need to be understood before determining whether the site should be trusted. If you do not know of a legitimate reason why the certificate cannot be verified you should not submit information to the site.

1. Check if a digital certificate is present by checking that:
 - https appears in the browser address bar; and



- a padlock is present (the position depends on the browser being used);

2. If a certificate is present, check if the certificate is valid by clicking on the padlock to see if:

- the domain name listed on the digital certificate is exactly the same as the domain name in the address bar; and
- the certificate is not self-issued, ie not issued by the same entity that owns the web domain name; and
- the certificate has not expired.

Facts about SSL

Having explained what a digital certificate is and why it is important to check, it is relevant to explain what SSL can and cannot do.

a) When a web site's identity is verified by a trusted third party, evident by examining the digital certificate, it provides an assurance that the web domain name belongs to the entity claimed. In other words, it provides an assurance about the identity and authenticity of the web site and hence helps users decide whether the web site can or should be trusted, particularly if the user needs to submit personal or other sensitive information to the web site.

b) SSL encrypts the traffic in transit sent and received between your computer and the web site to protect the confidentiality of the data in transit only. This protection is particularly important when accessing the web site from an unsecured (unencrypted) WiFi hotspot. Without the presence of https (or with just http), it means the information is not encrypted and can easily be seen by others using the wireless (WiFi) network.

c) If one of the computers that participates in an SSL session is compromised with certain types of malware (typically a user's computer that connects to the web site with a browser), attackers may still read and capture the data *after it has been decrypted* on the user's computers *or before it is encrypted* by the user's computer and sent to the web site.



Myths about SSL

a) **Myth:** An SSL protected web site means it is a secure web site and less likely to be hacked.

An SSL protected web site provides no assurance about the security of the web site itself or how well those who manage the web site handle your personal information stored on its databases. An SSL protected web site is not necessarily more secure than a web site that does not use SSL. An SSL web site is no more or less able to be compromised or defaced than one that does not use SSL. *SSL mainly provides protection for data in transit only and allows you to verify that you are connected to the right web site, and not a fraudulent web site impersonating a legitimate web site.*

b) **Myth:** Attackers cannot see, access or capture or modify any information obtained or submitted during an SSL protected session.

See paragraph c above for an explanation.

Report updated February 2011