

STAY SMART ONLINE ALERT SERVICE

Factsheet 10

How to detect phishing sites and steps to prevent being fooled by them

Phishing attacks are a common form of attack used by cyber criminals to fool users to disclose sensitive personal or financial information, including account credentials, for fraudulent purposes. Typically, there are several new phishing attacks targeting Australian Internet users each week. Therefore, it is prudent for online users to understand what a phishing attack is and how best to protect against such attacks.

What is a phishing attack?

A phishing attack involves the use of a web site that has been set up by criminals to look like the web sites of well known organisations, such as Australian financial institutions or government agencies and has the aim of defrauding or stealing personal information from the victim.

A phishing attack has two main stages:

- Phishing email: The attacker sends a spam email to thousands of email addresses pretending to be from a legitimate organisation. The email is worded to persuade the user to click on a link in the email. If the user clicks on the link, the user's computer will connect to the phishing web site.
- Phishing web site: The phishing web site is created to capture any fields completed by the user (such as username and passwords). If the user completes these fields the information will be captured by the attacker.

If criminals are able to convince a user that its email and web site are legitimate they can trick users into providing their user names and passwords (or other sensitive information) to the web site, which allows the criminals to capture their credentials and use them for illicit financial gain.

1. The best way to avoid becoming a victim of a phishing attack is to detect and/or block the phishing email (which is the first stage of the attack) which includes a link to the actual phishing site.

- a. Use a spam filter to block spam email.

Phishing attacks generally rely on a user receiving and clicking on a link in a phishing email. By blocking and filtering spam email, users are less likely to read, trust or click on a link in a phishing email if it is blocked or marked as suspicious by a spam filter.

- b. Change settings on your email software to warn you when you receive a suspicious email that may be a phishing email.

Spam filters though very useful and highly recommended are not always completely effective and some spam may still arrive in your inbox. In these cases it is recommended that you configure your email software to warn you in the event that a suspected phishing email arrives in your inbox.

If you use either Microsoft Outlook Express (Factsheet 4), Mozilla Thunderbird (Factsheet 5) or Microsoft Live Mail (Factsheet 7), these factsheets provide guidance on how these email programs can be configured to warn you about potential phishing emails you may receive.

2. In the event that you are fooled by the phishing email (first stage of the attack) and inadvertently click on a link to the phishing site, it is useful to understand how to detect a phishing web site.

Detecting a phishing web site can be done by one of two methods. Neither method is completely reliable and hence it is recommended that both approaches be used for best results.

Firstly, users can configure their web browser to help detect phishing sites. Please note that like anti-virus and anti-spyware software, there is always a delay between when a new attack is released and when these security technologies are updated to detect the new attack.

Both Microsoft Internet Explorer version 7 and Mozilla Firefox version 2 have features which can be activated to help detect phishing web sites. Turning these features on is unlikely to have any noticeable impact on the speed of your Internet connection.

- a) In Microsoft Internet Explorer version 7, the phishing filter can be turned on by selecting "Tools" menu, then "Internet Options", then select "Turn on automatic website checking":

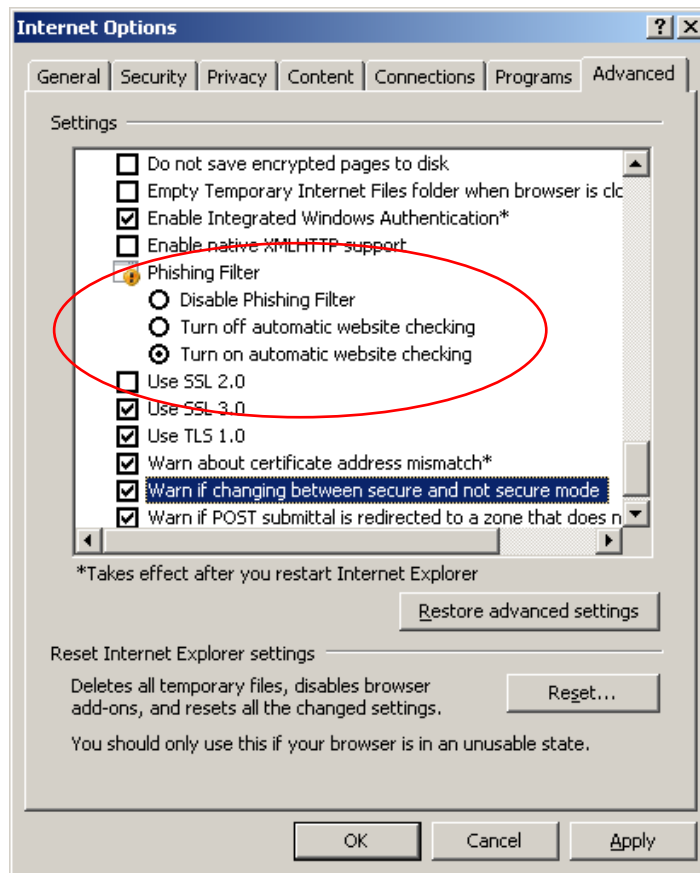


Figure 1, Ensure phishing filter is enabled

- b) Click "Apply" then "OK" to save these settings.
- c) In Firefox, click on Tools menu, select Options, select the Security tab then select the check box for "Tell me if the site I'm visiting is a suspected forgery". Either option is fine, however, according to the Mozilla Firefox help notes, the Google option will provide a more reliable check for you.

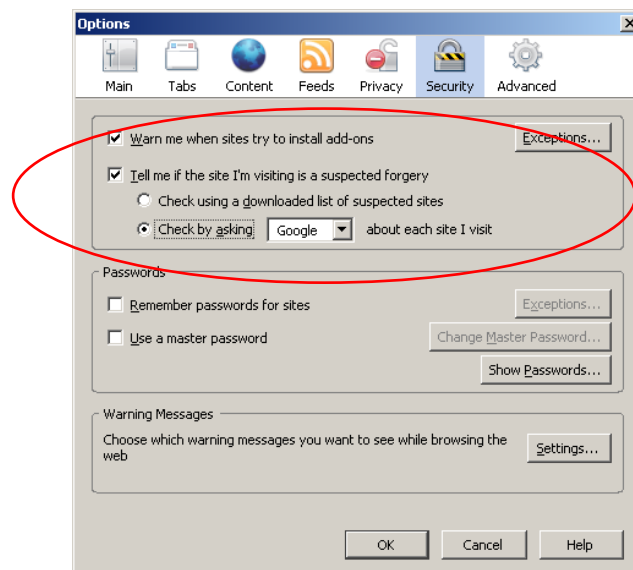


Figure 2, Firefox anti-phishing settings

See Factsheets 6 and 8 for more information about these features.

Secondly, users can look for the presence and validity of digital certificates on phishing web sites. See Factsheet 9 for an explanation of what features to look for.

3. What to do if you encounter a phishing email or web site.

If you receive a phishing email simply delete it. Do not reply to the email address and do not click on the link within the email body.

If you do happen to click on the link in the email body by mistake, do not "login" to the phishing web site or complete any fields on the web page which seek information from you.

Some phishing emails direct users to fraudulent web sites that also contain malware. Even if you do not "login" to the phishing site or supply other personal information to the site, just by clicking on the link, you may unwittingly install malware on your computer.

4. Recognising phishing emails and web sites.

The security technologies described above are very useful to help users protect themselves from phishing attacks. However, commonsense and user savvy also have a role to play when occasionally security technologies fail.

This section, therefore, seeks to describe some of the characteristics of phishing emails and web sites that will help users recognise them without relying on technology.

There are so many different examples of phishing emails and web sites that it is impractical to cover the full range of possibilities. However, phishing emails and phishing web sites have common characteristics.

Phishing emails generally contain the following characteristics:

- Email body purports to be from a well known organisation
- Email "from" field domain name may not be consistent with the domain name for the legitimate organisation¹
- It includes a web link within the email body
- The purpose of the email is to encourage the reader to click on the web link and login or provide other personal information.

Phishing web sites will generally have the following characteristics:

¹ Some phishing emails change the "from" field and insert the domain name belonging to the legitimate organisation. Hence, just looking at the "from" field does not always provide a clue that it is fraudulent.

- Web site appears to be the same as the web site for a well-known organization
- Some fields on the web page may not be the same as for the real site for those familiar with the real site
- Web domain and URL (in the address) bar is not the same as the web domain URL for the legitimate organisation
- Usually no https in the address bar, when it would normally be used for a login page (instead only uses http)
- Either no padlock, or incorrect placement of padlock on the web page instead of its usual position in the browser, or invalid digital certificate or self-signed digital certificate.

The Anti-Phishing Working Group and Miller Smiles have archives of phishing emails and web sites. Note these archives are mostly for US and UK based phishing emails and Australian Internet users are more likely to receive phishing emails pretending to be from Australian banks or financial institutions and sometimes, Australian government agencies.

The examples provide an explanation of the characteristics which indicate the email and associated web page are fraudulent and hence provide a useful way for users to learn to distinguish phishing emails and web sites from legitimate emails and web sites.

Anti-Phishing Working Group archive:

http://www.antiphishing.org/phishing_archive/phishing_archive.html

Miller Smiles archive: <http://www.millersmiles.co.uk/report/7062>

Report prepared May 2008
