



Factsheet 20 – Web threats – what are they and what you can do to protect your computer and information?

The purpose of this factsheet is to explain what web-based threats are, how they can affect online users and what users can do to reduce their risks while online.

Online threats are those related to being connected to the Internet or other networks. Online threats consist of many types, but well-known and common online threats are those which take advantage of email and web services. However, just connecting your computer to the Internet provides a range of other potential ways your computer can be attacked even when you are not using the web (through your web browser) or reading or accessing email. The purpose of this factsheet is to talk about web based threats specifically.

Web based threats

Web based threats fall into the following categories.

Phishing web sites

These are web sites which impersonate web sites that belong to well known organisations and brands. Criminals create the fraudulent web sites to try and trick potential victims to type in their username and password, or other sensitive information. Usually the criminal will send a spam email or SMS message or similar to potential victims to let them know about the web site.

Compromised legitimate web sites

These are legitimate web sites, belonging to legitimate organisations and businesses, which criminals have 'hacked' and use to host malware hidden within the code of the web page itself. The malware won't be visible but sometimes (not always) it may require the user to click on another link or button within the web page to activate the download of the malware to the user's computer. Sometimes the malicious code on the compromised web site might simply force the user's computer to redirect to another web site which hosts the malware and again the connection will generally occur in the background without the user's knowledge.

As with phishing sites, the criminals often send an email or some other message to potential victims with a pretext to induce them to click on the web link.



Unfortunately, there is also a trend for criminals to simply compromise legitimate web sites, and simply wait for ordinary users/customers or the public to visit the web sites of their own accord. The effect is the same whether the user was directed to visit the web site due to some false pretext in an email or other message, or whether the user chose to visit the web site of their own accord.

What can you do to protect against web based threats?

Firstly, you need to be following all the recommended security practices in the:

- [Secure Computer Checklist](#).

Enable and use limited user accounts for all users on your computer. Refer to the following factsheet for guidelines for Windows XP:

- [Setting up a limited user account in Windows XP](#)

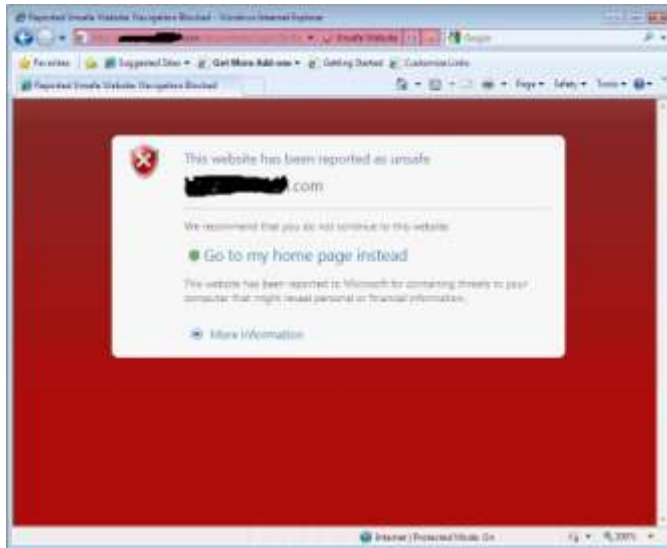
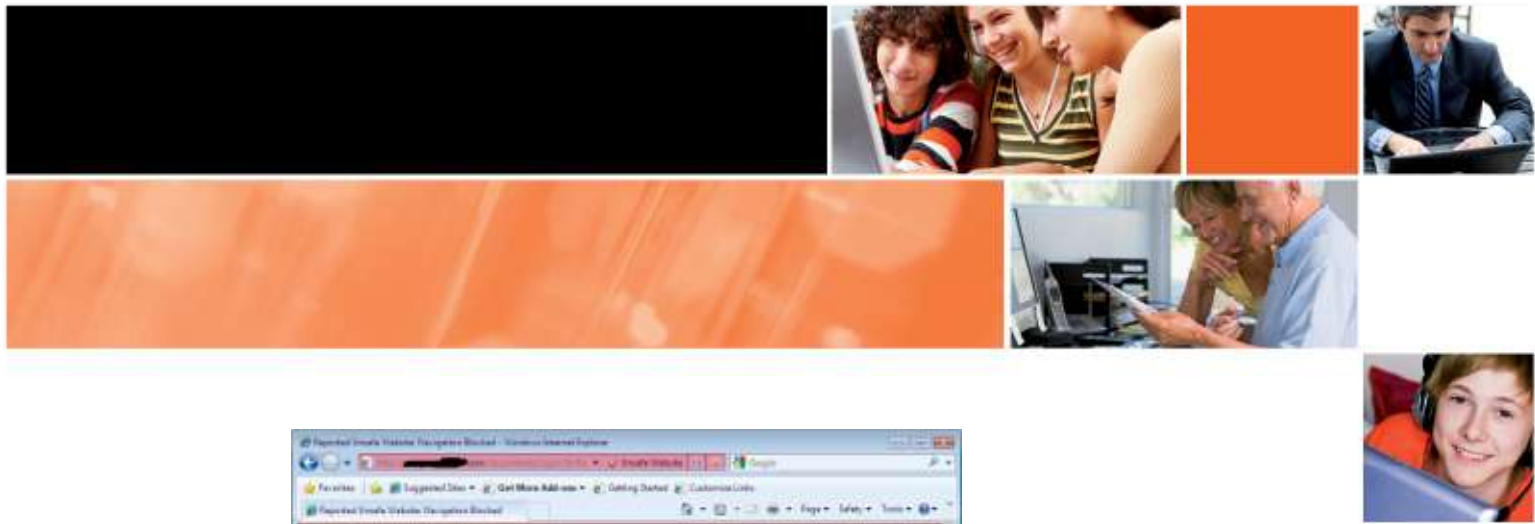
For tips to help you better detect and avoid becoming a victim of a phishing attack, read the factsheets about phishing:

- [Protecting yourself against phishing attacks](#) and
- [Understanding digital certificates and how they can help build trust online](#),

As your web browser is the computer's interface with the web and web-based threats, follow the guidelines for securing your web browser in the following factsheets:

- [Securing Microsoft Internet Explorer](#)
- [Securing Mozilla Firefox](#)

These features are available in most web browsers including Internet Explorer, Mozilla Firefox and Apple Safari. The settings can help provide warnings of potentially harmful web sites, such as the following example:



If using the Google search engine, Google may include a warning in the list of web link (URLs) search results which says: “ This site may harm your computer.”

Some Internet security programs, such as McAfee’s SiteAdvisor, or AVG LinkScanner, provide indicators of whether web sites, including within search engine results, are ‘safe’ or not. Usually safe sites are marked with a green tick or similar.

However, be warned that all these mechanisms have their limitations. They use a variety of methods to make an assessment about the safety, or otherwise, of a particular web site. These techniques are useful but not always reliable.

Like anti-virus software there is generally a delay between when the attack occurs (such as the web site is compromised to serve malware) and when the detection methods referred to above are updated to warn potential visitors to the site. As such, sometimes these tools give incorrect information, such as a green tick when the site has since been compromised, or a red cross even though the site has been fixed and removed the harmful malware.

Therefore, never rely completely on technology alone. Exercise caution and commonsense while online.

Report prepared August 2009