This tutorial has been produced by The Australian Tourism Data Warehouse as part of the complete online education program, Tourism e-kit

SECURITY AND BACKUPS

| **Reading time: 15 minutes**	**Prerequisite: n/a**

Since your online strategy is a core component of your business plan, you need to ensure that you are able to recover all your files should your website crash or your computer be attacked by a virus. This tutorial will take you through the steps to maximise your online and offline security.

1)   HOW CAN I TELL A (MY) WEBSITE IS SECURE?

If you are about to enter sensitive information on a page (such as your credit card details or login details to a bank account), you have to ensure that the page you are entering those details on is secure.

To do so, look for the signs:

- HTTPS instead of HTTP

- Locked lock
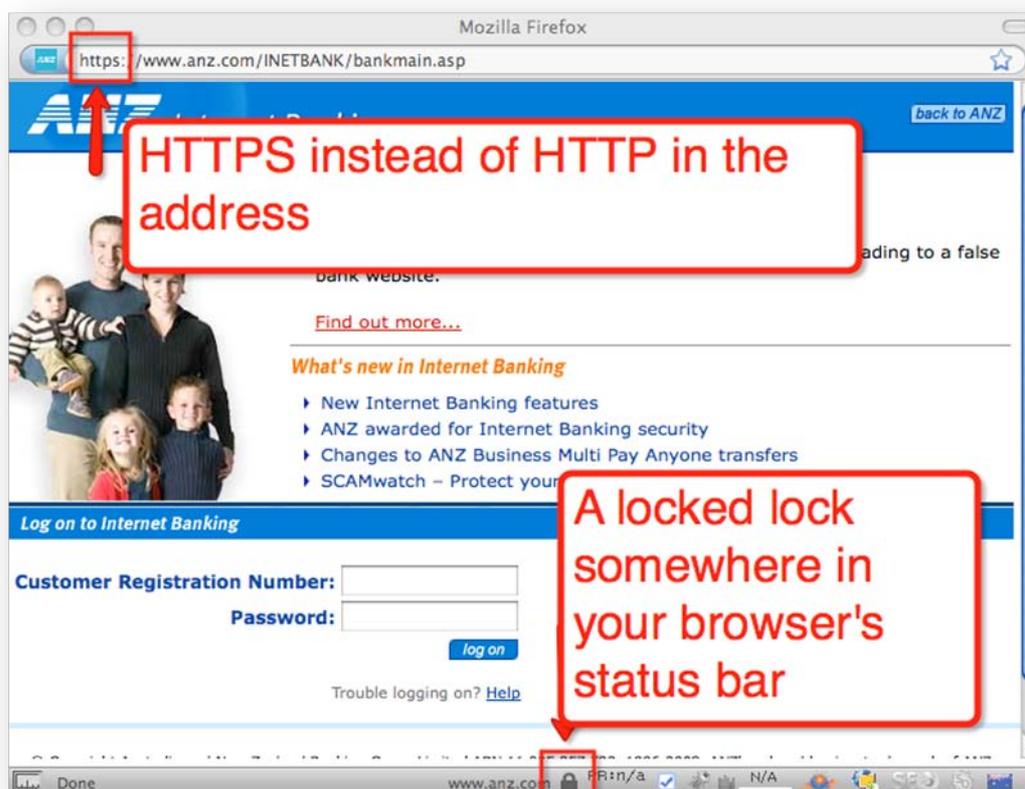
Screen capture copyright: ANZ

If you click on the lock, you will access information about the "SSL Certificate". The system that ensures a secure connection between your browser and the server it communicates with (in the first secure example the server is the ANZ bank) is called SSL. The HTTPS and the locked lock confirm the active SSL session.

You will find more information on this website: http://info.ssl.com/article.aspx?id=10068

2) IF I AM TAKING PAYMENTS ONLINE

If you are taking payments online you will be collecting credit card details. These details are actually being collected by the third-party online booking system you are using. For peace of mind, pretend that you are a client and check that both the HTTPS and the lock are present on the pages where sensitive information is required.

3) HOAX EMAILS AND PHISHING

A hoax is an attempt to trick an audience into believing something false is real. The process of sending fraudulent emails seeking personal information and claiming to be legitimate is called "phishing".

Emails claiming to be from PayPal, Google, eBay, YouTube or online banks are commonly used to lure you to a falsified website. For instance, phishers can ask you to enter your login details and then credit card information. They will copy these details and use them to log into the real website or empty your bank account.

A good example of a recent phishing scam was the Google AdWords phishing scam email:

Dear Advertiser,

We were unable to process your payment.

Your ads will be suspended soon unless we can process your payment. To prevent your ads from being suspended, please update your payment information.

Please sign in to your account at http://adwords.google.com/select/login

and update your payment information.

We look forward to providing you with the most effective advertising available.

Thank you for advertising with Google AdWords.

The Google AdWords Team

The link in the above email takes the user to http://adwords.google.com.**sesool.cn**/select/Login. The real address of the website (once you click on the link in the email) is not http://adwords.google.com but another site, **sesool.cn** which is pretending to be AdWords by adding the Google address before its name.

The AdWords phishing scam in explained in greater details on this Hoax-Slayer.com page: www.hoax-slayer.com/adwords-phishing-scam.shtml. Visit www.hoax-slayer.com to find out about the latest email hoaxes and scams.

### a)	What to do if you got caught

If you believe you might have been the target of a scam, follow these steps:

- Contact your bank **immediately** and cancel your credit card

- Change the password of the account that was phished **and** of every other account in which you were using the same password.

### b)	What can I do to avoid getting caught?

- Update to Internet Explorer 7 or install Firefox 3 from www.firefox.com as your default browser. Both browsers have built-in phishing protection that warns you when a site has been reported as fraudulent.

- Never respond to emails asking you for your credit card details or asking you to log in and update your credit card details.

- Never open a suspicious attachment

- Be wary and check www.hoax-slayer.com or copy and paste a few sentences from the content of the email into Google and see if any other Internet user has flagged this emails as spam.

## 4)	HOW DO I BACKUP MY WEBSITE?

Your web host will normally automatically backup your website (including files, database and email accounts) once a day and provide you with the backup to restore your site upon request. However, it is advised not to only rely on your host but either conduct your own backups or ask your web developer to regularly do so on your behalf. If you intend to do it yourself, read below.

### a)	Downloading my files via FTP

Your website is made of folders and files which are located on your host. You can access these via a very simple program called an FTP client. FTP stands for File Transfer Protocol.

Free FTP programs can be downloaded and installed within seconds:

- FileZilla: www.filezilla-project.org or SmartFTP: www.smartftp.com are for Windows

- Cyberduck: www.cyberduck.ch is for Mac

Once you are logged in (your host would have provided you with your FTP login and password) you can simply download a copy of your files to your hard drive.

If you do not have a content management system installed, you do not need to read below. All your content is located within your files and the backup via FTP is sufficient.

b) If I have a content management system

If you have a content management system, your content resides in a database (MySQL or Microsoft SQL Server) that is hosted on the server. **Your content isn't within your website's files**. Even though your host will backup your database automatically, it is a good idea to download a copy to your computer as well. Please also back up your files via FTP (see above) as the files form the mould in which your content will be displayed.

To backup your database, you will need your login and password to access your host's control panel.

If your database is MySQL you can follow the detailed steps listed here: http://fragments.turtlemeat.com/MySQL-database-backup-restore-PHPmyadmin.PHP

It is recommended to backup your database once a month and store the files on your computer.

5) HOW CAN I BACKUP MY COMPUTER AUTOMATICALLY?

It is much more likely that a crash will occur at your end than on your web server. In order to avoid losing all the documents and files stored on your hard disk it is **essential that you regularly back up your own computer.** Backing up a computer is something that is usually done automatically. All you need to do is spend a couple of hundred of dollars on an external hard drive, connect it to your computer and install the software.

You can also back up your files online, using systems such as www.jungledisk.com. It is very reliable and cheap.

Photo credit UntangleMyWeb.com

a) What to look for when buying an external hard drive

You can purchase your external drive from your local computer store or from electronics shop. However, prices may vary a lot so do your research. Also ensure your future hard drive meets the below requirements:

- Capacity: choose 500GB minimum (especially if you have lots of photos!)

- Connection between the drive and your computer: at least USB 2.0. Most of external hard drives now offer a faster connection than USB that is called FireWire. FireWire 400 is the standard but some drives offer FireWire 800 (faster). **Before buying the drive, check if your computer has a FireWire 400 or 800 port or both**. Then buy a drive that has the same port.

- Brand: ensure you buy a reputable brand. High quality hard drives are made by companies such as LaCie, Maxtor, Seagate, and Western Digital. Ask your computer professional for advice.

Photo credit UntangleMyWeb.com

6) RELATED MATERIAL

a) Related tutorials

- Organising hosting for my site