**Staying Safe**

1. The merchant is always responsible for security of the Internet-connected PC where customer details are handled. Virus protection and a firewall are the minimum requirements. To be absolutely safe, sensitive information and customer details should be stored on pendrives or a physically separate PC. Always keep multiple back-ups of essential information, and ensure they are stored safely off-site.

2. Where customers order by email, information should be encrypted with PGP or similar software. Or payment should be made by specially encrypted checks and ordering software.

3. Where credit cards are taken online and processed later, it's the merchant's responsibility to check security of the hosting company's webserver. Use a reputable company and demand detailed replies to your queries.

4. Where credit cards are taken online and processed in real time, four situations arise:   
a. Company uses an Internet payment service bureau. Sensitive information is handled entirely by the service bureau, which is responsible for its security. Other customer and order details are your responsibility as in 3. above.   
b. Company possesses an ecommerce merchant account but uses the digital certificate supplied by the hosting company. A cheap option acceptable for smallish transactions with SMEs. Check out the hosting company, and the terms and conditions applying to the digital certificate.   
c. Company possesses an ecommerce merchant account and obtains its own digital certificate. Check out the hosting company, and enter into a dialog with the certification authority: they will certainly probe your credentials.   
d. Company possesses a merchant account, and runs the business from its own server. Company needs trained IT staff to maintain all aspects of security — firewalls, Kerberos, SSL, and a digital certificate for the server.

Security is a vexing, costly and complicated business, but a single lapse can be expensive in lost funds, records and reputation. Don't wait for disaster to strike, but stay proactive, employing a security expert where necessary.

**Fraud Prevention**

Companies do not have to accept every online order, or not immediately. Escrow services are widely available. Trade associations and other institutions provide useful information and support. Payment service providers have levels of security. The order page can ask for further details, and its country drop-down list be amended to exclude the worst offenders. Affiliate businesses need to be especially careful, and in these ways:

1. Prevent competitors stealing their affiliate links by using inexpensive software for the purpose.  
2. Prevent bogus clicks-throughs by competitors who do not purchase but aim to bankrupt them with the pay-per-click search engines.   
3. Impression fraud by competitors aiming to lower their click-through rates and so disqualify their ads with Google.

The last two scams are often outsourced to low-wage outlets and/or employ special software. Companies need to track their clicks with special click auditing software (sometimes included in bid management software), or ensure that the company that runs their pay-per-click campaigns does so.

**Webpage Content**

Companies are responsible for the content of their web pages, which means ensuring:

1. Nothing is libelous or could be construed so.   
2. Material does not infringe copyright.   
3. Links don't damage the interests of sites linked to (deep-linking may).   
4. Pages don't fall foul of search engine and directory requirements.

America is a litigious society. Play safe, and even consider cloaking techniques to prevent information being extracted from pages and made the basis of frivolous lawsuits.

**Customer Data**

Companies are always responsible for customer information: an onerous task if it includes credit card and/or bank details. Use secure webforms that automatically transfer and store customer information safely on a third-party secure site. Encrypt it. Keep it off Internet-connected machines. Make several copies and store safely off-site. Seventy percent of companies that lose their customer data are reputed to go out of business within the year.

**Webservers**

Webserver security is highly technical, but you should should check or ask about:

1. The financial standing of the hosting company, and how long they have been in business.  
2. Security protocols to cope with denial-of-service and hacker attacks.   
3. Regularity of backups: does it include user logs, product databases, order tracking logs, server-side scripts, etc.?   
4. Ensure (www.whois.net) that you and not the hosting company remain the administrative and technical contact for your domain and — most critically — the registrant of the domain.   
5. Complaints procedure: you don't want your site dumped because of an unwarranted complaint from a competitor.   
6. Scrutinize the contract (and employ a business lawyer to check copyright, complaints, fees and service renewal / discontinuation matters).

**Viruses**

Computers need to be kept free of viruses and spyware by running the appropriate software regularly. The firewall settings also need to be checked periodically.

**Online Storage**

You may wish to store highly confidential information (passwords, bank accounts, etc.) on password-protected directories on your PCs, but do ensure you encrypt the files first.

A better solution is to employ professional online storage facilities, which offer various levels of security. They are not expensive, and some ISPs offer limited storage free to customers. Particularly useful are services that allow customer-sensitive material to be sent directly from your web pages and stored in a secure facility for later processing.

**Legal Matters**

Your company is bound by the laws and regulations of the state or country in which it is incorporated. Check that you understand the basics, and have experts to consult if and when needed. Be especially careful of material that could offend the authorities or religious groups abroad, be considered inflammatory, or supportive of outlawed or terrorist groups — i.e. keep your social and political aspirations for another site and another name.

**Disaster Recovery**

Some hosting companies offer a disaster recovery service — usually at a steep monthly price — but the best approach is to prevent disaster striking in the first place by following mandatory routines. Nonetheless, if the unthinkable does happen, all is not necessarily lost.