

UnderstandIT

From **MAY DAY CONSULTING LIMITED** in association with **FACILITATORS UK**

A publication designed to inform and enable businesses to understand the implications, costs and advantages of using Information and Communications Technology. Distributed through Chambers of Commerce.

E-COMMERCE – TURNING POINT IN CONFIDENCE?

A number of major online retailers have reported a boom in online sales, particularly over the festive season. For example, both Amazon and Tesco.com have announced significant increases in online business during the past 2 months. Many other “e-tailers” are also saying that their online businesses have been overwhelming their back-office support staff and many have had difficulty in meeting the demand.

This underlines the increasing consumer confidence in using the Internet for their personal-to-business and business-to-business transactions.

On the other side of the coin, there has been a major increase in online fraud and so-called “identity theft”. We have probably all received an email purporting to be from a bank, asking us to click on a link contained within the email to visit the bank’s web site. You are then directed to enter personal information “to ensure that your account is updated and does not expire”. The site visited is usually a cleverly constructed copy of the real bank’s site and the unsuspecting consumer’s account details are harvested and it will soon be emptied. (See December 2004 edition on “phishing”).

Some in the IT security sector estimate that the incidence of such criminal activity is on a similar trajectory to that of the commerce itself – up!

It is also clear that organised crime has now become involved in many of the international scams that have been seen in the past 6 months. As a result, because of the resources available to organised crime, there is a similar increase in the level of sophistication applied to the various scams. The skills of hacking, virus development and email spamming can now be applied jointly to perpetrate ever-more complex scams on unsuspecting consumers and businesses.

It is true that many of the major viruses that have appeared in the past couple of years have not been developed by organised crime, but the methodologies used by the misguided individuals involved are now almost certainly being employed to develop a network of “sleeping proxies” – infected PCs that will be dormant until required and then used to provide a channel for launching fraud attacks and acting as a screen to protect the perpetrators.

Lack of education and awareness leaves consumers extremely vulnerable and will need to be continually addressed in the coming months and years.

All this sounds very frightening, and in future, it will almost certainly become a much higher profile issue both for large and small businesses, and their consumers. However, it is not all doom and gloom. As discussed earlier, many businesses are benefiting significantly from increased e-commerce activity, and this success will inevitably continue.

At the same time, much work has to be done to protect us all from cyber criminal activity and the onus is on government, the IT industry, businesses and consumers to ensure that we are all increasingly aware of what is happening and how to avoid becoming a victim.

MICROSOFT RELEASES BETA VERSION OF NEW SPYWARE SOFTWARE

Microsoft recently acquired a company called GIANT that specialised in producing anti-spy ware software. Microsoft has now released a beta (test) version of a new product that uses the GIANT database technology.

This is the latest attempt by Microsoft to help users to combat threats to their computing environment. Many blame Microsoft for the many supposed flaws in their Windows operating system technologies. It is true that there are security flaws in many Microsoft products, but MS has a good track record in releasing fixes for most of them immediately and at no cost to users.

In fact, threats from “spyware” are not indicative of shortcomings in Microsoft’s software. They derive from attempts by many large international corporations (as well as smaller ones) to invade our “cyber-space” in an attempt to advertise their products and services, usually in a devious way.

The beta test version of the new software is freely available for download. However, initial reaction from many users is that there are still a few “bugs” that need to be resolved.

One unresolved issue is whether Microsoft will be charging for the final product, when it is fully tested.

For the not so feint-hearted, the beta software can be downloaded for free from

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

The message from Alan Finch of May Day Consulting is that it works (it caught about 3 or 4 missed by other free products), is easy to set up and well worth a trial; at least whilst it is free.

ICONS, ICONS AND MORE ICONS...

There are many ways of launching a program within Windows, and without some thought, your computer can end up being very cluttered and untidy.

When installing new software, you often have the option of choosing where you want to place “shortcuts” to it. There are basically three places:

- The START menu (conventionally, **all** programs are shown here)
- The desktop
- The Quick Launch bar

We often see the desktop of many of our clients’ computers completely covered in icons, and often they do not understand why they are there or what to do with them.

An icon, whether on the desktop or in the Quick Launch bar, is just a shortcut to the program itself and deleting it will NOT delete the program. So, where should you place icons or “shortcuts”? This of course is purely personal choice, but if you are not disciplined, then your computer can become untidy.

You can place icons pointing to frequently-used programs on the Desktop yourself if you wish to have quick access to them without going through the START menu. Whether you do, is purely a matter of personal choice and convenience.

A quick way of placing an icon on the desktop is to go to the START menu, select the program concerned and right-click on it. This will produce a menu of options, one of which is SEND TO. Click on this and select DESKTOP (Create shortcut). You will now have a shortcut to the program on your desktop.

Similarly, shortcuts to programs can be placed on the Quick Launch bar. This is an area on the Task bar immediately to the right of the START button, (usually on the bottom of the Windows screen) – see below:



If this bar is not visible, then you can make it so by right-clicking on the Taskbar. Make sure there is no check mark against LOCK THE TASKBAR, then select TOOLBARS and check the QUICK LAUNCH item.

To place a program icon here, you can drag an existing icon from the desktop and drop it on the Quick Launch bar. Alternatively, you need to go to MY COMPUTER and find the program itself under the application folder under the PROGRAM FILES folder.

The program file is usually the one with a .exe extension or with the main program icon adjacent to it in the list of files in the application folder. Click on the program file and drag it onto the Quick Launch bar. This will create an icon and it will now appear on the bar.

NB: The Quick Launch bar does not automatically re-size when you add icons. You can manually make it longer by dragging the divider to the right.

CHIP AND PIN TECHNOLOGY

Whilst this subject is not strictly an IT issue, we feel that it is important that small businesses who accept credit card payments for goods or services should understand the implications of the current changes to the responsibilities between card issuers, businesses and their consumers.

There appears to be some confusion, particularly with small businesses as to exactly what the changes that have just come into effect mean to them. There are also a few “grey” areas that need clarification.

With effect from January 1st 2005, the responsibility for fraudulent use of credit cards falls on the retailer or organisation accepting the card in payment for services, and NOT the card issuer.

However, this assumes that the card terminal has been upgraded to accept the new Chip and Pin credit and debit cards. If the terminal has not been upgraded by the card issuer or bank, and this is due to no fault on the part of the terminal renter or business concerned, then responsibility for any fraudulent use of cards will continue to lay with the card issuer.

Similarly, if the card provided by the consumer has not been replaced with a new Chip and Pin card, then responsibility also still lays with the card issuer.

On the other hand, if the card tendered is a Chip and Pin card, but the consumer does not have, cannot remember, or insists on signing the credit card slip, then responsibility for fraudulent use will lay with the retailer or business concerned and NOT the card issuer.

Further information on these and related issues concerning the new credit card technology can be found at:

<http://www.chipandpin.co.uk/index.html>

In addition, the Federation for Small Businesses has issued a press release that attempts to explain some of the issues. You can see it at:

<http://www.fsb.org.uk/news.asp?REC=2261>

We wish to acknowledge with thanks that some of the material contained within this publication has been sourced from Computer Weekly.

May Day Consulting Limited and your Chamber of Commerce have endeavoured to ensure the accuracy of the information contained in this publication, but do not accept liability for any inaccuracy or omission contained within it.

Information on other Business and IT services can be found on our web site at: <http://www.maydayconsulting.co.uk> or by calling Alan Finch on 07968 262079.

May Day Consulting Ltd

....stress free IT

9 Benbecula Road
ABERDEEN AB16 1FT
Tel: (01224) 697457

E-mail: info@maydayconsulting.co.uk
Internet: <http://www.maydayconsulting.co.uk>