



# Information Communications Technology Newsletter

Issue: February 2009

Editor: Stanley M Debono

Foundation for Information Technology Accessibility

Improving the quality of life of disabled persons through ICT.

## Contents

Welcome to the 62<sup>nd</sup> issue of the FITA newsletter.

Email the editor on [stanley.debono@gov.mt](mailto:stanley.debono@gov.mt)

- 1) Website of the month - Commercials for the family computer
- 2) Question Box - How do I secure my laptop?
- 3) Articles - Interactive White Board: A Powerful Pedagogical Innovation for Classrooms
- 4) Credits
- 5) Disclaimer

## Website of the month

### ++ Commercials for the family computer

The last time I visited the site it was highlighting the commercials for the family computer - the Commodore 64 and video of Carnival at the 1941 Mardi Gras in New Orleans. Those topics will probably not be of immediate interest to you. They are an example of the variety of content you will find at the Archive.

Movies, pictures, audio, text, software, and more. All of it free and all of it legal. You can spend a lot of time just getting used to the place.

Maybe the coolest section of Archive.org is the WayBack Machine. This page relies in part on Alexa Internet to serve up pages from the past. Type in a familiar URL and you can look at what was displayed at this address in days of yore. I tried it with The Naked PC site and smiled as I witnessed visual recollections of the old web page formats we used as we

tried to come up with a look we liked, that was easily maintained. Or take a look at Microsoft's home page circa 1996. Fun stuff." One of my favorite uses for the WayBack Machine is to locate lost web pages/sites. You may have experienced this sometimes -- You are clicking through a site and start coming across "File Not Found pages. This can be because, links can be pointing to deleted or renamed pages. Next time that happens to you, head over to the WayBack Machine. Most of the time you will find exactly what you are looking for.

You can find the Internet Archive at: <http://www.archive.org/> You will see the WayBack machine near the top of the page.

## Articles

### ++ Interactive White Board

A Powerful Pedagogical Innovation for Classrooms - The Interactive White Board is emerging as a useful tool for the classroom for teacher input to the

whole class. But it's easy to develop a view on the form factor (It's a must-have tool / its too expensive, etc) rather than on what it is capable to achieve inside the classroom.

Like any other tool, it is only as good as the outcomes it can produce in a classroom. Hence the right questions to ask are -'Does it increase engagement of students in the classroom? Does it improve understanding and retention of concepts? Does it improve the critical thinking skills of students?' Can it be adapted to involve all students and cater for their learning needs?

But all this shall not happen on its own. It has to be managed as an overall programme with well defined timelines, measurement and course correction (if required). It is important to carry all stakeholders in this journey, including parents and school management. There is a tipping point for technology in classrooms, where a critical mass of teachers have started experiencing the benefits of technology and are able to assume the role of attracting other teachers towards their approach.

There are some pitfalls to avoid. Using technology is essential in the early stages, its important to give hands-on experiences with the Board to teachers, so that they do not remain armchair critics. The initial success is because of the fact that the White Boards are reliable and easy to use and in continuity to the existing chalk and talk method. Thus, teachers are enthusiastic about the possibilities of technology and are inspired to use ICT often in curriculum delivery. The single large visual focal point in the classroom is a strong magnet to attract and retain student attention and motivation towards the lesson.

But using the Board in the classroom is no guarantee for a sound pedagogy. The sound pedagogical principles have to be built on top of the basic functionality of the Board. Making the class to think, involving them in collaborative work, correlating the curriculum to the student's daily life have to be fostered by the creative use of software functionalities on the Interactive Board. It is important to help teachers use the pace and flow of lesson delivery through the use of ready-made models / diagrams / animations, so that time can be freed up for teachers to focus on discovery based learning scenarios in their classes. Overall, the Board is a great tool for the constructivist educator.

Above all, we believe there is no 'one size fits all' approach at work here. It is better to inform the teachers about the creative possibilities of crafting engaging/visual and interactive lesson plans, to give them raw material to build such lessons and then allow them to make final choices on how best to create the lesson and to involve the students in the classroom. This choice has to be with the teacher

For more hands on practical resources, you may wish to start at <http://iwb.org.uk/>. This is a rapidly growing bank of free to use tools and resources created for teachers who are teaching with an interactive whiteboard (IWB).

All the resources have been contributed freely by their creators and may be used freely within educational establishments. Please read both our copyright page and disclaimer.

Contribute any of your own resources and help this bank to grow. All contributions will be fully acknowledged.

Read more at: <http://iwb.org.uk/>

*Source: Rohit Pande, CEO, classteacher Learning Systems  
Contributed by: Stanley M. Debono*

## Question Box

### ++ How do I secure my laptop?

Keeping your laptop or netbook safe involves a combination of common sense, physical security devices, and software strategies. Let's start with devices that make it harder for your portable computer to be carried off by someone else.

#### + Security Hardware

Physical security devices are used to keep your laptop from being stolen or used without your authorization. The most basic physical security device is a laptop security cable. This cable connects to your laptop and secures it to a non-moveable item in your office, hotel or conference room. For example, you can connect your laptop to your desk, or the leg of a conference room table. The cables usually have a combination or key lock device, and attach to the security slot found on most notebook computers. A determined thief with a bolt cutter could foil this device, but it certainly makes it a lot harder to grab and run.

Another physical security device that you can add to your laptop is a theft protection tab. This tab is used to identify the owner of the computer and to prevent people from trying to resell your stolen computer. If this tab is removed then it leaves a permanent acid "tattoo" on the laptop, and in some cases it can also damage the LCD.

These security tabs are available from STOP (<http://www.stoptheft.com/>).

Biometric devices can also be used to ensure that if your laptop is stolen, it can't be used by someone else. Biometric devices include fingerprint scanners and retinal scanners. These devices can be added to just about any laptop. As at date of publication, the fingerprint scanner comes standard on some Toshiba laptops.

#### + Security Software

Front Door Software's Retriever software can help to get your laptop back if it's lost or stolen. Retriever displays ownership information at startup, and can also report tracking information to the owner if the laptop goes online. Also, if your laptop is stolen, you can login to the Front Door website and enter a lockdown code that will help to protect your information. You can even send a personal message to the thief, or cause an audible "This laptop was stolen!" alarm to be played. Retriever works on XP, Vista, Linux, and Mac OS X. The software has a 90-day free trial.

Lojack for Laptops is another software-based laptop recovery product. This company provides you with a Theft Recovery Team that's actually a licensed private investigation agency. They will work with local (US) law enforcement and Internet Service Providers, using information sent from the stolen computer, to assist local police in recovering your computer. They claim that 3 out of 4 stolen computers with Lojack for Laptops are recovered.

## **++ File Encryption**

Of course, there's the threat of hackers and snoops that attack through viruses and spyware. Every laptop should have an up-to-date anti-virus and anti-spyware software package installed, to identify and remove malware from your system.

File encryption is used to protect your data from hackers, thieves and others who may access your computer without permission. It is usually done by special software programs, however, Windows XP offers a free encryption tool that you can use to protect individual files and folders.

If you have Windows Server 2008 or Windows Vista (Ultimate or Enterprise edition), BitLocker can be used to encrypt an entire hard drive.

Other options for encryption are PGP's Whole Disk Encryption (Microsoft and Mac OS X), and the free TrueCrypt software, which can encrypt a hard drive partition, USB flash drive or external hard drive. TrueCrypt works on Windows, Mac and Linux systems.

## **++ Password Security**

In addition to physically securing your laptop and protecting your computer with security software, you also need to take steps to protect your laptop with strong passwords. While it is important to set up a user account password for your laptop you will also want to set up a power-on password. These passwords will prevent

unauthorized people from logging in to your computer, or accessing it by using a boot-up disc. To create your and power-on password you will need to enter your BIOS security set-up menu.

This is usually accessed by pressing the Del, F1 or F2 key while your computer is starting up. Try to use passwords that include a combination of at least eight letters and numbers, and stick to a password rotation schedule that changes your passwords on a regular basis. Make sure you remember the passwords, or you'll lock yourself out!

*Also be sure not to make other changes to settings within the BIOS screens, or your laptop may fail to start.*

Here's one other point on passwords, particularly relevant for travelers. If you allow your web browser to store your passwords, and your laptop is stolen, you've given away the keys to the kingdom.

Roboform and similar tools can keep all your passwords handy, but with the protection of a master password.

To keep your laptop as safe as possible you will want to combine physical, software and use password strategies. While not all of the above security methods are applicable, practical or necessary for all laptop users, it is still important to understand what your security options are so that you can alter your security strategies as your computer use evolves.

## **Credits**

FITA's services are made possible thanks to the support of the following funding partners.

- Malta Information Technology and Training Services Ltd.
- National Commission Persons with Disability
- Gasan Group of Companies
- Computime Ltd.
- Philip Toledo Ltd
- Megabyte Ltd
- The Computer Society of Malta
- SMS Group of Companies
- Crimsonwing (Malta)
- 6PM Consultancy Group
- Engineering Centre

## **Disclaimer**

The reader is responsible for the use of information contained herein and its safe and lawful use. This includes work policies and restrictions applicable to the computer environment specific to the user. Descriptions of products or services are for information purposes only.

FITA makes no claim, representation or warranty, express or implied, as to the information presented here, the performance of products and services, or any results that may be obtainable by their use. FITA also does not necessarily endorse the specific content or positions contained in the articles shown or referred to.