Issue 184

JANUARY 2014

ISLE OF WIGHT PC USER GROUP

IWPCUG

HOT KEY

WINTER 2014

In December Dennis Linzmaier gave us an interesting talk on Steganography, followed by a quiz.

In This Issue Pages

The Isle of Wight Personal Computer User Group

We welcome anyone who has an interest in computers and related technology and what you can do with it.
We are a group which seeks to exchange ideas and new information.
Membership is £12 per annum

Our meetings are held on the first Wednesday of each month at
The Riverside Centre, Newport from 7.30 to 9.30 pm
Visitors are welcome.

A charge of £2 is made per meeting, which includes tea or coffee during the break.

If you would like to know more about us, you are most welcome to come along to one of our meetings, or you can contact one of our Committee Members listed on page 3.

The Club Website address is **www.iwpcug.org**
We also have an e-group discussion area on
Yahoo groups: **iwpcusers@yahoogroups.com.**

FUTURE MEETINGS

Date	Subject	Speaker
January 8	**DirectX & PC graphics**	**Richard Burkhill**
February 5	**AGM**	

ISLE OF WIGHT PC USER GROUP COMMITTEE

Chairman : David Groom

Treasurer : Phil Rogers

Secretary : Susanne Bone

Membership and Database Secretary : Roger Skidmore

Committee Member : Steve Sutters

Committee Member : Soren Johanson

HotKey Editor : Bob Groom

Note:

Contact details removed prior to publishing on the internet

Suggestions for new events, topics or speakers for talks are always welcome.

Please contact Steve Sutters, or any committee member, with your ideas.

If necessary we may be able to find a speaker for your subject.

Chairmans Report

Firstly may I wish you all a Happy New Year, and best wishes for 2014.

After a few years of things remaining relatively quiet for home computing, we already know that 2014 will see a major shift when Microsoft abandons support for Windows XP. See more about this on the next page.

Our AGM is next month, I already know of at least one committee member who is stepping down, and there may be others. To avoid too much falling onto the shoulders of the remaining committee members it would be nice if we had at least one new face decide to put their name forward for election.

The events calendar on page 2 may be looking a little thin, but we do have some events under discussion, so keep an eye on the club web site and egroup for confirmation of these. It was pleasing to see two new speakers talk at our October & November meetings, and hopefully we may be able to get them to come along again this coming year. We are, as you may well know, always on the look out for new people to come and talk, have a word with Steve Sutters if you know of someone.

David Groom

Car Sharing / Lifts

It is possible that a number of our members do not attend our monthly meetings because they find transport to Newport difficult and the committee have wondered if it might be possible to arrange lifts for those members. With a membership as large as ours it is not always obvious who might like to attend but has difficulty with transport, and secondly, who might live nearby and be able to offer them a lift.

As a first step, if you would like to attend the meetings, currently can’t get to the Riverside Centre on a Wednesday evening and would like to see if there is a nearby member who might offer you a lift, then could you please get in contact with me. We will then try and find a member who might be willing to give you a lift.

David Groom

The End of Windows XP

By the time you read this, there will only be about 4 months until the support for Windows XP ends. After April 8, 2014, there will be no new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates. Microsoft will also stop providing Microsoft Security Essentials for download on Windows XP on this date.

Although the Windows XP operating system is now over 12 years old, I know a number of us are still using it, so what does the end of support mean for us?

Firstly it is important to realise that your computer will not stop working, and in fact you should really not notice any immediate changes at all. However the risk of running an operating system (and if you use Internet Explorer - a web browser) for which there are longer no security patches should not be underestimated.

I have to admit I still use XP, and not a week goes past without there being a new patch from Microsoft to fix existing security issues. One very real problem is that the prevalence of exploits against Windows XP may will increase after this date. As soon as Microsoft releases security updates for supported versions of Windows, attackers will reverse engineer those updates, find the vulnerabilities and test Windows XP to see if it shares those vulnerabilities. How often could this scenario occur? Between July 2012 and July 2013 Windows XP was an affected product in 45 Microsoft security bulletins, of which 30 also affected Windows 7 and Windows 8.

Another cause for concern is that security software vendors will likely stop patching, updating and supporting versions of their software which runs on XP.

What should you do?

1) The only real safe thing to do is to finally decide to upgrade Windows XP to either Windows 7 or 8.

2) If you can't move away from XP, then at the very least you must ensure that all updates which have been released prior to April 8 are installed, and that the anti-virus software you are using will be continued to be updated for new threats.

Other Important Points to Consider

So far I have only considered the threat from malware, but there is another looming problem. How many of us have ever had to reinstall Windows XP? We probably have the original installation CD, and hopefully Service Pack 2 on a CD, but having installed those we would normally go online and download and install all the updates. Microsoft have stated that existing updates to XP will still continue to be hosted after April 8. As a precaution I would at least recommend downloading XP Service Pack 3, (a 316Mb file available http://www.microsoft.com/en-us/download/details.aspx?id=24) and burning it to a CD and storing it with your Windows XP installation disks. You may also want to consider downloading and storing the various updates which have been released by Microsoft for Windows XP since SP3 was issued.

Microsoft have also said Windows XP activation will be unaffected by the Windows XP support end date. Therefore if you need to reinstall XP you will still be able to legally activate the Operating System.

David Groom

Tip :

If you want to download windows update files then have a look at this article http://support.microsoft.com/kb/323166

Working at Bletchley Park

The following article is abridged from the speaker notes produced by Albert Bareham prior to him giving a talk to the IWPCUG in 1999. Although we have heard some of what was undertaken at Bletchley during WW2 I have decided it worthy of inclusion since we are fortunate to have a first hand account of what went on there. I hope to publish the full text of the speaker notes on our web site.

The earliest recorded reference to codes/cyphers is in Babylonian times - Most of these Egyptian - Greek Babylonian have been broken in recent years - there are still a few which have not been cracked. There are records dated 1324 that King Edward 11 had all messages coming from or destined for Foreign parts intercepted and passed to the "Intelligence Officers" of the time.

If you fancy a long read for the winter months get "The Code Breakers" by Kahn from the library – it’s about 3" thick and is fascinating reading.

In 1939 I was working in the Engineering Department of the Post Office on telephone switching systems - at that time entirely electro-mechanical, principally relays, when an Order in Council was made closing down all amateur radio transmitters and I found myself part of a team visiting radio amateurs and confiscating their equipment - my part was to certify that the equipment was capable of transmitting radio signals; we also took away state-of- the-art receivers Halicrafters, H.R.O., Eddystone, etc. which were to play a significant role in the story of Bletchley Park (“B.P”).

I continued to work on various security classified projects until early 1942 when I received "The note" - I was to report to the Director of Research, Dr. Radley, at Dollis Hill Research Station in north-west London. Three of us arrived and were told to go away and come back the next day when there would be three more arriving from Scotland. We were interviewed as a group and then the security check was put in hand. In the meantime we were given various jobs to do in the Laboratories, mainly developing circuit elements using valves, which at the time we were unaware were later to be incorporated in Colossus. After some weeks we were assembled in Tom Flower's' office, signed the full Official Secrets Act and then told why we were there.

The details of the Enigma machine in use by the German services were already known and German messages were being intercepted; many were decrypted but it was a slow process. An equipment called "Robinson", no doubt you can guess why, had been developed at T.R.E. to mechanise the task of finding the wheel settings of the machine (each of the German services used a variant of the basic Enigma machine). This machine aptly named was slow, clumsy, and relied on mechanical relay technology. Initially I worked on a replacement version where valves replaced relays. I should perhaps have mentioned that code breaking relies heavily on statistical techniques and hence the need to count and record was important. The ring counters used thyratrons GTIC (gas filled relays), high speed relays and finally conventional Post Office type relays. When the count stopped the state of each ring was fed to a relay tree via cathode followers and then to a numeric display.

There were earlier equipments, e.g. "Bombes" which were electro-mechanical, very noisy and slow but for all that played an important part in finding wheel settings.

The need to read messages at High Command level (which we knew by the code name "Fish") between Hitler, Goering and their generals was paramount. They used a more sophisticated system, developed by Lorentz -the Geheimschreiber based on the SZ40. The Germans believed this to be totally secure. Unlike the Enigma machines which used 3 to 5 wheels the Lorentz had 12 ,and the possible combinations is enormous, billions in fact. To find the wheel settings was the task of the equipment which became known as Colossus.

In February 1943 amidst great secrecy the small group led by Tom Flowers who was around 35 at the time, and the rest of us in our early 20s worked in a secure room 12 hours a day, 6 1/2 days a week, to create Colossus Mk.1 - about half the size of the partial replica of a Mk.2 which some of you saw at Bletchley. When Tom Flowers proposed the concept of Colossus there were many sceptics who were sure that although it might work in principle it would be unreliable because of the 1,500 valves. In 1938/9 Tom Flowers had been working on the idea of an electronic telephone exchange using valves and had shown that providing the voltages used were conservatively rated and more importantly once they were switched on they were not turned off, a high degree of reliability was achievable - fortunately Tom Flowers argued his case convincingly and the go ahead was given (I believe that Winston Churchill personally gave the order that the utmost priority was to be accorded to the project - any components we requested and test gear e.g. oscilloscopes, AVOs etc., appeared as by magic.) In a relatively short time it was built and tested to specification. We dismantled it into transportable units and took it to BP, Block F. Reassembled and tested to the design parameters it was ready for a live test using real traffic on 8th December 1943 - it worked!!!!!! The cryptographers were delighted with their new toy but immediately the Oliver Twist syndrome surfaced. Can we have more, and we want it to be capable of performing additional functions; hence the idea of Colossus Mk.2 was born. This met the additional requirements and used 3,500 valves. The reliability was even greater than had been predicted and on 1 June 1944 the first one was operational. It was five times as fast as Mk 1. By VE Day I believe we had 10 or maybe 12 Mk.IIs operational.

Colossus was the first practical application of a large scale programme control computer, the sequence of operations i.e. the programme was controlled by setting external switches (Key & Yaxley) and plug boards by Wrens on the instructions of the Duty Cryptographer.

In February 1944 the Germans further modified the Lorentz machine with a view to making the system even more secure but in fact it made it easier to crack. With 'D-Day' imminent breaking of the German High Command traffic was crucial but Colossus ensured that the main link between Berlin and Field Marshall von Rundstedt, the Commander in Chief of the German forces in the West was continuously broken. It has been estimated that the intelligence obtained shortened the war by 2 years and saved between 2 and 3 million lives.

With the approach of victory the German threat receded and increasing numbers of staff were moved to Japanese Section. At last VE day arrived for which we had striven so long and patiently - a strange atmosphere pervaded the Station - Messages in German plain language began to arrive. Commander Travis, Head of BP issued a special order to all staff expressing thanks for the dedication and effort. He ended with a reminder that "The temptation now to 'own up' to our family and friends as to the nature of our work has been and is a very real and natural one. It must be resisted absolutely.

Tom Flowers received an instruction that all traces and references to Colossus must be destroyed. Tom took the drawings to nearby Woburn Abbey, the majority of the Wrens were billeted there, and burnt them in the furnaces while we broke up the equipment. The Head of our section was Max Newman, Professor of Mathematics at Manchester University and a few panels were salvaged and formed the basis of the computer which the University developed.

In 1943 (maybe 1944, my memory is not all that good) we were joined by a small group of Americans (I believe as a result of one of the regular meetings between Churchill and Roosevelt). It has now been revealed that the Americans were given copies of the drawings. In the 1970s some information about Colossus was released - this took the Americans by surprise for they had claimed that they had invented the world's first electronic computer ENIAC. (Electronic Numerical Integrator And Calculator). Another example of how great British inventions were given away and exploited by another country. The rebuild of Colossus did not involve our BP Group as we were still 'silenced' - I believe Tony Sale and his collaborators in the project obtained their information from American Government sources under the "Freedom of Information Act". When we visited BP I concluded that there was much work yet to be done and the information they had was far from complete.

Despite the long hours we worked I enjoyed my involvement in the project and am grateful that I was selected to be part of such a great achievement.

Sadly Tom Flowers died recently at the age of 93, active to the last, and the world owes so much to him - for his work in creating Colossus he received a MBE, in my view a damning commentary on the Honours system when footballers, pop stars, actors, etc. receive knighthoods, CBE's and the like. It was ever thus, engineers never were and still are not recognised as the greatest economic asset a country has - they are the true creators of economic prosperity. Tom began his life as a Dockyard Apprentice, obtained a BSc. degree then joined the Engineering Department of the Post Office. After he retired he received a Doctorate for his work.

<u>Tidbits:</u>

Now a few short notes that you might find interesting.

After D Day BP decrypted around 18,000 messages each day.

Colossus was a universal machine which performed operations logically rather than mathematically. Given various inputs it would convert them into outputs depending upon the programme. Present day computers are purely serial and this explains why when programmed to do the same operations as Colossus, that, in spite of the increase in speed, they still take approximately the same time to do the job.

Two now well-known personalities I remember at BP were Ian Fleming, a young officer who subsequently became famous as the author of James Bond and Roy Jenkins a young graduate, now a famous Politician.

I hope my talk has given you some idea of the background of Colossus and what it achieved.

Albert Bareham (27 August 1999)

NOTICE OF AGM

Notice is hereby given that the Annual General Meeting of the Isle of Wight PC User Group will be held on Wednesday 5th February 2014 at 7:30 PM at The Riverside Centre, Newport.

Nominations are requested for the positions of: Chairperson, Treasurer, Secretary, Membership Secretary, and up to eight other committee members.

Please send your nominations to the Secretary, Su Bone. Seconders are not necessary at this stage.

ISLE OF WIGHT PC USER GROUP
ANNUAL GENERAL MEETING AGENDA

1. Approve the minutes of the previous AGM, held on 6th February 2013, (http://www.iwpcug.org/secure/minutes/AGM2013v1.pdf)
2. Matters arising from the minutes.
3. Receive reports:
    - 3.1 Chairman
    - 3.2 Treasurer, including approval of the Club Accounts
    - 3.3 Secretary
    - 3.4 Membership Secretary
    - 3.5 Other activities: Computability, HotKey, Cover Disk, Website, Egroup, Marketing, Riverside Liaison
4. Elect a Chairperson, Treasurer, Secretary, and Membership Secretary.
5. Elect other Committee members (up to a maximum of eight persons).
6. Set the Annual Subscription.
7. Appoint an Independent Examiner.
8. Any Other Business.

Joining the Yahoo Group

Send an email to: **iwpcusers-subscribe@yahoogroups.com** with “join” in the subject line.

All members are encouraged to join this group (which costs nothing and is private to club members) in order to keep in touch with events and to join in with the discussions.

You can also keep in touch by regularly visiting **www.iwpcug.org**

Office Suites Can Be a Sweet Deal

One of the greatest inventions since the personal computer is the personal computer office suite. These software collections can handle most productivity tasks of a typical small or home office user or home user. Deals can be had.

All major office suites include at least a word processor, spreadsheet program, and presentation program. Depending on the suite and the version, a suite can also include a database program, photo editor, desktop publishing program, diagramming program, math program, and more.

Integrated software for the PC has existed since close to the beginning of PCs, with Lotus Symphony for DOS being the first popular PC suite, introduced in 1984. Claris AppleWorks for the Apple II computer was also released that year.

Microsoft began blowing away the rest of the office suite market in 1990 with the introduction of Microsoft Office in versions for Windows and the Mac. Today Microsoft Office remains the market leader by a wide margin.

In recent years, however, Microsoft Office's market strength has coalesced around the "enterprise," typically large companies who buy in bulk through site licenses. Microsoft Office today is a lot like IBM in the past, for whom the motto "You can't go wrong with IBM" existed in the minds of management information systems buyers.

Microsoft Office has a 90 percent share in the enterprise market, according to market research firm Gartner. Few large firms even consider other office suites, only 6 percent of the companies surveyed, according to another study by market research firm Forrester.

After a long run, Lotus SmartSuite, a successor to Lotus Symphony, was withdrawn from the market this past June. WordPerfect Office is still around, though barely, with only 1 percent of the enterprise market, according to Forrester.

Things are more interesting with small and home office users, home users, and students. A movement is afoot toward other office suites, with LibreOffice and Google Docs being the most popular alternatives. Each points to interesting personal computing trends. LibreOffice is free for all users, Google Docs for most users.

LibreOffice (www.libreoffice.org) is traditional software that you load from your computer's hard disk, except you install it by downloading from the Internet instead of copying from CDs. LibreOffice is "open-source" software, meaning that anybody with the programming skills can share in its development. Its past is almost as interesting as its present and future. LibreOffice is based on OpenOffice, launched in 2002 by Microsoft archrival Sun Microsystems as a free alternative to Microsoft Office, which was and remains expensive compared with most other software. LibreOffice was officially released in January 2011.

As the most popular open-source office suite, LibreOffice is made available by the Document Foundation, a nonprofit organization that has received funding from companies such as Google, Novell, and Red Hat.

LibreOffice is available in versions for Microsoft Windows, Mac OS X, and Linux. It consists of a word processor, spreadsheet program, presentation program, database management program, drawing program, and math program.

The positives to LibreOffice are its quality and comprehensiveness, Microsoft Office compatibility, and free cost.

The biggest negative to LibreOffice is that it's not 100 percent Microsoft Office compatible. Complex formatting in particular can get mangled if you open a document using Microsoft Office that was saved using LibreOffice.

Google Docs (docs.google.com) is "cloud" software that you can access only through your web browser when connected to the Internet. It consists of a word processor, spreadsheet program, presentation program, drawing program, and forms program.

Launched in 2007, Google Docs is available to users of any Internet platform and is the most popular cloud office suite.Google Docs is free for individual and educational users, with fees for business users starting at $5 per month.

The biggest positives to Google Docs are its portability and security. You can easily work on documents using different computers from different locations, and you can easily collaborate on documents in real-time with other users. It automatically saves documents to prevent data loss.

The biggest negative to Google Docs is its relatively poor compatibility with Microsoft Office. It's also not as feature rich as LibreOffice. If you lose your Internet connection, you can't use it.

Apple has an equivalent to LibreOffice, Apple iWork, for users of its OS X and iOS operating systems, though it's not as robust. Apple recently began offering iWork for free to buyers of new Apple computers and devices.

Microsoft has an equivalent to Google Docs, Microsoft Office 365, that like Microsoft Office is relatively expensive. The charge to enterprises is $20 per user per month.

Karen Hammond

Upgrading to Windows 7

Well, I've finally done it. I think. I am now typing this in Windows 7. Everyone said it had to be done so here we are.

Making the big leap forward depends on where and how you want to jump. If you just run a bare-bones installation on a simple computer with the minimum of software then with a shiny new hard disk it's no big deal. Copy your "My Documents" folder to USB stick, take out your old hard disk (you surely don't want to overwrite it, do you?) pop in the new one and run Windows 7 setup disk.

Follow any instructions, including your own Wi-Fi settings then copy your "My Documents" contents from your USB stick to the new "Documents" folder (under e.g. C:\users\roger\documents). Install Open Office and away you go. Well, don't forget your anti-virus software.

Unless you're me In which case you have lots of old programs (which necessitate 32 bit installation), three hard disk partitions (for the tidy-minded) and are a total back-up freak. My computer is a bit like a universal toolbox. So far the only advantages of upgrading to Win 7 have been that I can use a solid state drive and everybody says I have to upgrade. The disadvantages have been that I have had to deploy numerous work-arounds to achieve the same functionality. There's very little I can't now do after much effort and some expense (having to pay for upgrades or alternatives to some of my favourite programs), and some things are now more effort than before.

I still can't get my head round "Libraries" but fortunately I have discovered my favourite (free) file manager (XplorerLite2 by Zabkat) has folder bookmarks so I can get straight to the "libraries" as folders on my hard disk - in a file manager view. Phew!

I much preferred working in Win XP, even with an old style hard disk (mostly using "sleep" instead of "shut-down") but one has to yield to peer pressure - and I suppose I do feel a tiny bit more secure.

Roger Skidmore

P.S.
for other backup freaks - I use Acronis 11 whole disk clone and SyncBack for incremental data backups.

Paying, and Getting Paid, Online

Conveniently and inexpensively transferring money, whether as payment for goods or services or as a gift to family members or friends, is one important use for the Internet today.

Bitcoin (bitcoin.org), the largest decentralized electronic payment system currently in operation, made headlines recently.

In testimony before a U.S. Senate committee in November 2013, the general counsel for the nonprofit Bitcoin Foundation admitted that Bitcoin is "a high-risk environment, and potentially it's not quite ready for mass consumer adoption."

Bitcoin is "virtual currency." Anybody can buy Bitcoins using traditional currency such as dollars, euros, and yen, use them to buy goods and services, and exchange them for traditional currency. Their value, however, fluctuates wildly. When Bitcoin emerged in 2009, Bitcoins sold for less than a dollar, while recently the value of a single Bitcoin exceeded $650, and six weeks before that it was valued at only $110.

Because the use of Bitcoin is anonymous and because Bitcoin isn't regulated by any governmental authority in the U.S. or elsewhere, Bitcoins are also used on the "Darknet" for the purchase of illegal drugs and weapons, forged documents, hacking services, child pornography, and hit men as well as for money laundering and other illicit activities.

In October 2013 the FBI shut down Silk Road, one Darknet market where Bitcoin was used heavily. One of Silk Road's nicknames was the "eBay for drugs." The Treasury Department is calling for regulation of virtual currency such as Bitcoin.

Finally, and this is what was behind the testimony of Bitcoin lawyer Patrick Murck before the Senate Homeland Security Committee, if you don't know what you're doing, Bitcoin can be a way for you to be parted from your money, cheated by a scammer.

On the positive side, the use of Bitcoin comes with lower merchant fees than are charged by credit card companies as well as low currency exchange fees, and it can be especially beneficial to consumers in developing countries who have little access to banks and other financial services.

The biggest name in the online payment market remains PayPal (paypal.com), which has been owned by Internet auction behemoth eBay since 2002. Whereas Bitcoin is largest decentralized electronic payment system, PayPal is the largest centralized electronic payment system, or "payment service provider," and is much more mainstream.

Using PayPal, an online merchant can accept payments for goods or services without a credit card merchant account and the fees associated with it, which can amount to as much as 5.5 percent of sales for a small business.

With a PayPal account, individuals can make Internet purchases without a credit card and without incurring charges for PayPal use. Individuals can also use PayPal to receive money from a family member or friend without incurring fees so long as the funds come from the sender's bank or PayPal account instead of a credit card account. Using Western Union for such a transfer within the U.S. leads to charges of $8 to $12 on a $100 payment.

PayPal generates most of its revenue from charges to online merchants. For most transactions within the U.S., the fee is 2.9 percent of the transaction plus $0.30, with large companies receiving discounts depending on sales volume. In 2012 PayPal generated a whopping $5.6 billion in revenue.

PayPal has safeguards to help protect buyers and sellers from fraud. Buyers have 45 days after a transaction to report that an item bought through PayPal hasn't arrived or that the item is "significantly not as described" -- different, broken, or counterfeit, for instance.

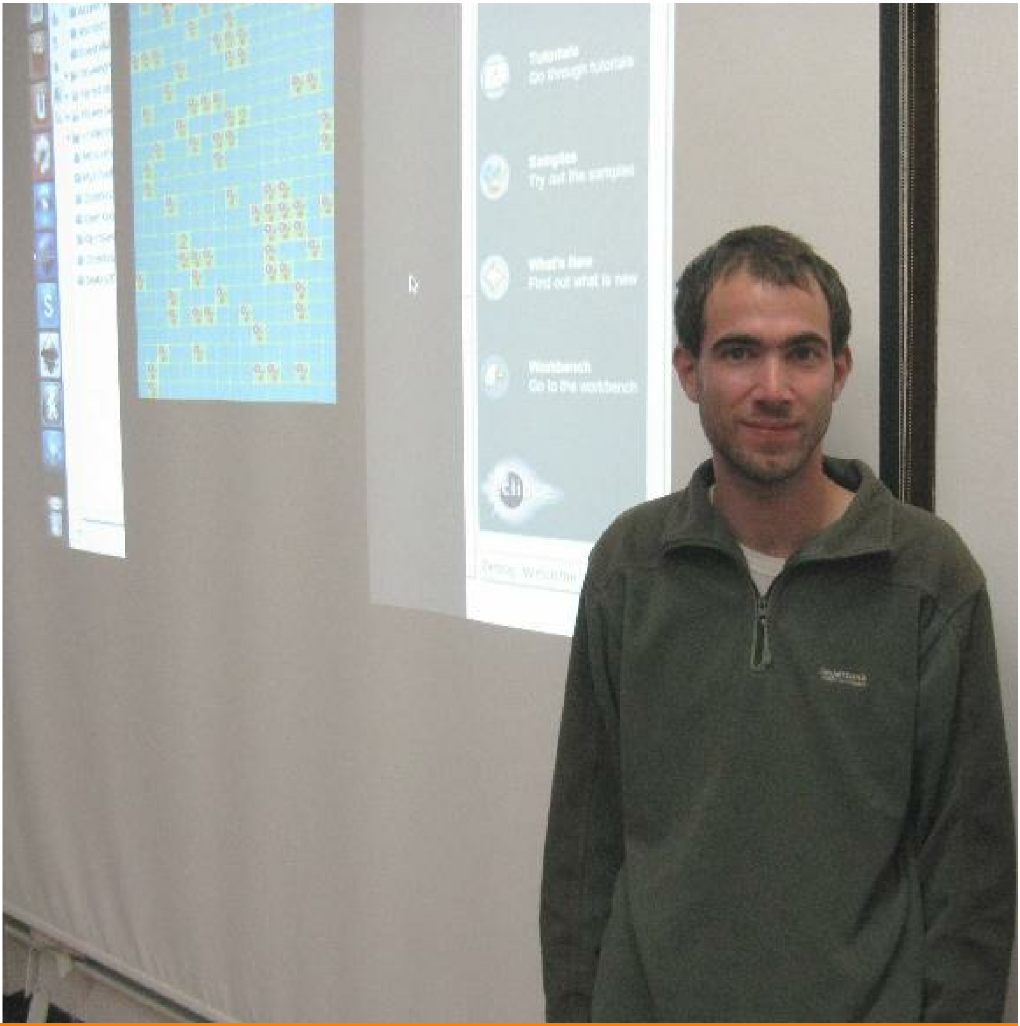
Sellers have protection against fraudulent chargebacks when a buyer falsely claims that an item sold didn't arrive. But sellers have to provide a high standard of proof that any item they sold did in fact arrive.

To help prevent problems with the use of PayPal, you should take precautions. Log directly onto PayPal's website rather than clicking on a possibly bogus link in an email message, even if the email looks legitimate or looks like it came from a legitimate sender.

Beware of spoof websites with names such as PayPai that try to trick you into revealing your PayPal password. Don't use the same password for your PayPal account as your email account.

Bitcoin and PayPal aren't the only games in town. Several dozen other digital currencies exist, though most are similar to Bitcoin. Big Internet players such as Amazon with Amazon Payments and Google with Google Wallet also act as online payment service providers, as do a host of smaller companies.

Karen Hammond



In October Richard Valvona demonstrated the principles of programming using the game of minesweeper as an example.

We try to publish HOTKEY quarterly in April, July, October and January
This edition was compiled using Serif PagePlus 9
and printed by Island Printers, East Street, Ryde.

No responsibility can be accepted with respect to any advice or suggestions in this journal.