A Season of Happiness   Focus Special

THE CYBER MINEFIELD
!!! it's out there !!!

the dangers of taking the Internet at face value

It comes from the nowhere, it goes to the no-place, and here it is: that self-serving ethereal world of the Internet. Since its creation, at least as far as we users are concerned, it has wheedled its way into our lives and we are becoming ever-more reliant on it. At first we were sceptical, but the Frankenteins who created it told us it was perfectly safe and we believed them, the same way we accepted the reassurances of their physicist cousins who discovered nuclear fission. What are we - naive, stupid, or simply desperate to embrace anything new for fear of missing out on the benefits? Make no mistake, there are advantages, perhaps some way beyond comprehension; but they come at a price, one we would do well to consider before we accept total domination by this awesome dictator.

The amazing thing is that a tool so powerful can spring from something as small as a silicon chip. If rumours are true, the next stage will be the nano-dot, a component invisible to the naked eye which can store massive amounts of data and increase the speed of computer modules phenomenally. Big deal, you might say - more power to us, and you will probably be right. But think about this - even employing the sophisticated technology of today, a complex security password might take years to crack; with the nano-dot, the same code could be broken in just hours! Then, your PC, laptop, Ipad and tablet, even your mobile phone, are virtually open books for anyone to browse, copy and download from. So much for safe!

My main concern is how far and fast this cyber invasion is spreading. Bad enough that personal information can be poached and used for identity theft. This kind of crime not only costs money, then the time to repair any damage, but afterwards the victim is left feeling insecure and despoiled as if their home has been broken into and their personal belongings rifled through. How much worse is it when the sanctity of family and relationships is compromised? It can happen, it does happen. The Internet makes it very, very possible.

In a few cases, infiltration of our systems is perpetrated by a group of geeks with amazing programming skills and motivated by some immature compulsion to create havoc. Following their touch of insanity, our computers go haywire, sometimes crash completely and often present us with puerile comments and even images of a silly or obscene nature. The bugs and viruses that inflict this disruption to our routine, though temporarily inconvenient, are rarely regarded as little more than nuisance value and are quickly remedied by a reliable security manager. Anyone who doesn't have one to guard their system should invest, pretty quick smart, because the dangers from hackers are going to increase. And it won't necessarily be the kind who are just out for a bit of fun. Hacking is big business offering huge rewards for the scammers, high costs for their victims.

Not so long ago, an Australian home-owner went overseas for a lengthy period. When he returned, his house had been sold without his knowledge or consent and the elaborate deception had been engineered over the Internet by someone in Nigeria! How they achieved this seemingly impossible deception, I have no idea. Presumably, whatever loop-hole they found hadn't been anticipated by those who'd set up the system in the first place. Needless to say, questions were asked and embarrassed authorities were racing around like crazy to plug the gap and make sure the same thing never happened again. Unfortunately, it will, somehow. Cyber criminals know that pickings via the Internet are easy when their marks are so trusting and complacent. It's money for nothing, and the click's for free!

How do they manage it, though, when there are supposed to be all these security measures in place to safeguard users? We think we've figured out one way following a recent problem which, fortunately, only affected our private email service. I don't know what scam the perpetrator hoped to pull, but all of our contacts received an email claiming to be from us and containing a link to click on. One of these emails was actually received by us purporting to be *from* us! We were onto it straight away and sent warnings to everyone telling them not to activate the link. As far as we know, no-one has, so this particular scam hasn't worked; but it set us wondering how the cyber-crim had acquired our list of contacts in the first place. You see, we don't keep an address book on-line for security reasons. The only place the information could have come from was the folders containing old emails either sent or received and being held by our service provider. I'm not suggesting they were at fault, knowing the level of security they employ. It could have happened on one of those occasions when our screen froze while trying to log out, during which time someone may have broken in. Whatever, we then had the unenviable task of going through the back files - hundreds of them! - deleting the unnecessary ones and copying those containing important information before deleting them as well. In future, our email account will hold no emails in or out, and we certainly won't be setting up an address book. And now, the moment the screen locks up, we simply disconnect the Internet immediately.

Does it really matter? It might, especially if those links mentioned could have opened the door to the system of whomsoever clicked on them. Once in, the alien program could quite easily download all data and transmit it back to the source - details including private, business, banking and so on. The lot gone in the blink of an eye. Can you stop it? Well, maybe not forever, but there are precautions everyone can take to minimise the risk. Passwords are one way. Most of us already use them in some form, for example the PIN to access card accounts. Wherever possible, set up these security codes as front-line defence, prohibiting unauthorised progression past that point - no password, no entry! Be very canny about creating them. Avoid using standard words, names, birthdates, etc. And unless you want to have a bit of fun in the process, don't bother with the old spy trick of using the text from a book. It's confusing and unnecessary...

This code-maker is easy, it can be used over and over, and it can't be cracked except by pure chance (or a code-breaker using a nano-dot!). Mark, then cut out 80 small squares from a piece of card - a cornflake packet will do. Write each letter of the alphabet in lower case, but leave out 'o' - it's too easily confused with the number '0' which will also be omitted. That gives you 25 squares. On the next 25, write the upper case letters, minus 'O'. On the final 30, write numbers 1 to 9 and substitute a dash (-) for zero, this times three. Now all you have to do is place the lot into a suitable container, shake them up, pick one, record it, then drop it back in and shake again for the next character. The string can be as long as allowed and is likely to contain an assortment of upper and lower case letters along with numbers and maybe the odd dash. If you want more dashes, just mark and cut some extra squares. Because the characters are selected at random, there will be no predictable association by you or anyone else. Just make sure you keep your new password safe, or you'll lock yourself out as well!

Passwords and codes, no matter how complex and seemingly indecipherable, should be changed on occasions, preferably on a date also selected at random. Stay clear of the beginning and end of the month and, unless absolutely necessary, don't be on-line when you do this. The other way to stay safe is to sign up with a reputable security manager. Most offer varying levels of service, including the facility to customise your defence against unwanted contacts. Even then, some suspect communications can slip through like the example already mentioned. When in doubt, look at who it's from. Do you know them? Now check the subject matter. Does it have any relevance for you? If it is something vague like: Hey!, Hi or Hello, it's likely to be bogus. Don't open it - just delete it. And definitely don't click on an attachment to a suspect email! The main recipient will obviously be you; but when you open the email there may also be a string of other names. This means the same email has been sent to them as well. If you don't know the sender, be immediately suspicious. Even if it is supposed to be from a friend, ask yourself whether they would send a batch email, or forward one from another source? In future, ask your contacts to be specific with their introductory data and save the comic stuff for the email content. And you do the same for them.

Thanks to the Internet, social communication has been revolutionised. We can have video calls and conferences with people all over the world in real time; or we can chat on-line to friends in the next suburb, even a sister in the bedroom down the hall. It's truly amazing, a convenient way to keep in touch when a person-to-person meeting is impractical. Good, yeah? Well, it could be if everyone was respectful of everyone else and emotions never played a part. Unfortunately, the opposite is frequently true, especially on those social media sites where there is no video link and the written word alone says it all. You'd think it would serve people better, being able to review a message and edit it before sending, so avoiding the repercussion from words spoken in haste. But do they take the opportunity to keep life simple and relationships on an even keel? Young people in particular don't seem to worry about it, not at the time. They type their message sometimes faster than they can speak, a miracle in itself, and send it straight away without considering that it might offend or upset in its present form. Crash, bang - another friend gone! Too late to un-say what has been said. And what about Twitter - or should it be Twit...Der? In this arena, it would seem age is no barrier to stupidity and the sending of dumb, incautious comments!

Of course, misunderstandings happen every day, with or without the Internet, and if they were all we had to worry about, life would be less of a trial; but there are more shadows than a few in the cyber chat-room, some so dark that the evil intent hiding within is almost impossible to recognise until it strikes. Facebook is one of those sites offering both benefits and disadvantages. In the early days, even though they didn't understand it sufficiently to use it themselves, parents probably welcomed it as a diversion that kept the phone bill down. But in recent years, these chat-rooms have spawned an enigma we can well do without. So many young people are developing complexes instigated by comments posted on their pages, hate-filled messages and in some instances bare-faced lies, which undermine their self-esteem and paint a distortion of their personality that they themselves start to believe. The results are devastating, in a few instances fatal. You can't blame Facebook, nor most of the others like it. The element responsible is a cowardly minority which uses social media to inflict hurt, sometimes in a criminal way.

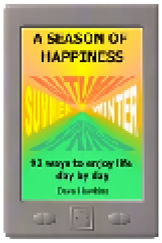
The problem is that they are throwing dirt while remaining unseen, immune to any reprisals other than by a counter-attack in the same format they used to deliver their assault. It sounds like a battle, a war, and it is, but it is being conducted in a way that is still relatively new to us and which is writing its own rules as it spreads. I don't know the answer. I doubt there is one that will satisfy the majority. We probably just have to live with it and help the impressionable grow thicker skins and encourage their self-worth. Once they know who they truly are, the hurtful opinions of others will have less impact.

This on-line bullying is a form of cyber-terrorism, employing psychology as the weapon of destruction. Attacks of this nature exploit the weaknesses of the target using the Internet as cover. There is, however, a greater danger which is not as obvious because the approach is nice instead of nasty. I am referring to the strategy of the cyber-predator. They pretend to be who they are not for the express purpose of luring the victim to an eventual face-to-face meeting. I still find it hard to believe how people can be so naive as to fall for this con. After all, they must know that an on-line profile could be pure fiction - they've probably exaggerated a bit in their own biography. So, why do they simply accept any new contact as genuine? The young boy or girl from across town might actually be cute and interesting as the text and picture suggest; but they could also be as old and ugly as the intentions in a predator's twisted mind. Please beware of taking this road to a dream. Sometimes there is no way back.

I apologise for raking through the negative side of the Internet, but it had to be said. As long as we are aware of the pitfalls, the benefits of using this wonderful medium are boundless. It does bring families and friends together in a way that letters and simple phone calls cannot. Life is made considerably easier when you can buy on-line, anything from a TV programme to a world cruise. Want to know something? Just Google it. You can even check out your cousin's house from across the road via a satellite picture. Who knows where this amazing technology is going? We will find out, in years to come. But let us never forget: we will always be the Masters, while it must only ever be our servant.

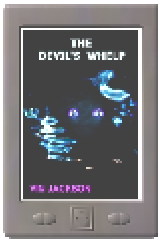
Our eBooks are available now in formats to suit popular eReaders, PC and Mac

The must-have Self-Help eBook

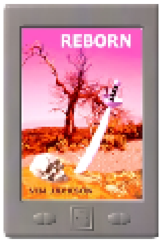


Romance/ Suspense

Horror



Heroic Fantasy



Visit the eBooks section to read the obligation-free, extended previews and get a good feel for the books before you buy. Or you can send one as a gift to a friend. Just click on the direct link to your favourite eBook store to see how.

Where every effort has been made to be accurate and fair-minded, comments and opinions expressed on this website are based on personal experience and do not necessarily reflect the views of the wider community or those groups and institutions mentioned. A Season of Happiness and its staff accept no responsibility for any outcome based on suggestions offered. What works for us may not work for you. Please bear this in mind.