ISSN 1466-9358 online

MMIT
Multimedia Information & Technology

Volume 42 Number 5 Spring 2017

■ Digitising the House of Lords' papers ■ Engaging parents with school libraries ■ Innovation in Brazil ■

welcome

This is my last issue as managing editor; after eight years I've thoroughly enjoyed, the time had come to make a change. The journal is also undergoing a change, moving to an open access model later this year.

Warm regards,

Cathie

Catherine Dhanjal, Managing Editor

From time to time, MmIT offers space to suppliers who are developing and marketing products of potential interest to information services. Neither the journal nor the MMIT Group endorse any of the services covered in these pages. Articles published reflect the opinions of the authors and are not necessarily those of the editorial board or MMIT Group. While every reasonable effort is made to ensure that the contents of the articles, editorial and advertising are accurate, no responsibility can be accepted by the editorial board or MMIT Group for errors, misrepresentations or any resulting effects. Acceptance of an advertisement does not imply endorsement of the advertiser's product(s) by the editorial board or MMIT.

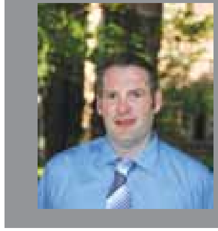
MmIT is published by the Multimedia Information & Technology Group of Cilip in electronic open access format from June 2017

Find out more about the change of editor and change to open access on page 3

Editorial enquiries to:

Leo Appleton
Interim Editor

Email:
l.appleton@gold.ac.uk



contents

Cover image: https://pixabay.com/en/users/intographics-2633886/

technology roundup

Practical security advice

Each passing day, more of us increasingly use the internet to send money and make purchases.

Keeping our connected devices secure is becoming more important. Here I share general best practice advice for preventing you becoming a victim of computer fraud which does not require much technical knowledge.

1. **Keep software updated**
Running the most recent versions of your mobile operating system, security software, apps & Web browsers is among the best defences against malware and other threats. When you see a message on your computer or mobile to update, then do so immediately. These updates often contain security patches which protect against new vulnerabilities.

2. **Use different passwords on all sites - and change them frequently**
Hackers often steal a login and password from one site and attempt to use it on other sites. To make it simple to generate – and remember – long, strong and unique passwords, it is good practice to install a reputable password manager which will create complex strong passwords and store them in an encrypted file on your own computer. You then only need to remember one Master password and the password manager will automatically take care of logging you into different sites with secure passwords.

3. **Use an ad blocker**
Believe it or not but there are a lot of malicious ads that can cause your device to become infected. Using an ad blocker on your browser can prevent these malicious ads appearing. It also speeds up browsing so you will experience quicker loading of websites. It is a win win but unfortunately, some websites require you to turn it off to see their content.

4. **Register with www.haveibeenpwned.com**
This is a legitimate website which collects all the emails associated with publicly known website hacks. Here you can submit your email to see if your personal details have been released in previous website hacks and you can also register your email to receive future notifications if your details appear in a future hack. If you do find your details registered, then login into the site where you were compromised and change your password. Watch out also for phishing emails from the site just hacked

5. **Look for a secure padlock icon in your browser**
This icon to the left of your URL signifies that the website is using https. Https is ‘secure http’ which ensures an encrypted connection is active so that your sensitive information like credit cards or passwords is not ‘sniffable’ by a hacker who is snooping on a network between you and the legitimate website. Not

all websites support https now but you should expect all sites which accept payments to have https enabled.

6. **Double-check the domain name of the website**
Always check before entering sensitive information to make sure you are not on a phishing website like paypa1.com or g00gle.com. You should also never click on a link in an email telling you to login to your sensitive accounts to resolve an issue. Instead, leave the email and go directly to the site and login. Links in emails which look legitimate can reroute you to rogue sites which capture your login details.

7. **Enable two-step authentication when offered**
Many sites such as Apple, Microsoft and Google now ask you to associate a mobile phone with your account. Two-factor authentication does not let you login without access to your mobile phone and this ultimately makes it much harder for an attacker to hijack your account (as they do not have your mobile phone to change account details).

8. **Do not click on anti-virus popup windows**
This is a common scam which tells you that your computer is infected with a virus. Genuine antivirus software does not do this. The popups install malware onto your computer, with your permission. Many now require you to pay money to have the software removed by the software originator. Malware such as Cryptolocker are a nightmare and are unremovable without paying ransom.

9. **Change default passwords**
Whenever you buy an Internet Connected device e.g. router, baby monitor, connected CCTV - change the default password. In fact, every device you purchase which has a default password should be changed on first use.
There are search engines like Shodan (https://www.shodan.io/) which crawl the web for connected IoT devices and hackers will try default passwords on those devices. You are basically leaving your keys in the door.

10. **Close out old accounts**
They simply create more points of vulnerability. Sometimes that might mean having to go through steps to recover an old password you might not remember, but it is worth it. The less footprint you have online, the better in general.

11. **Review your online accounts and credit report**
You should review your bank accounts, auction accounts, and mobile phone accounts for signs of fraud or charges that you did not make. Make this a regular habit. Yes, banks and credit card companies are quite good at spotting fraud but ultimately, it is up to you to spot fraud on your account.

12. **Treat public WiFi differently**
You should not use public WiFi hotspots without using a VPN connection. A VPN will encrypt your communications to and from the internet to prevent eavesdropping. At home or on wireless networks, where you enter a password, the connection is encrypted so that your information is not sent ‘in the clear’. Just be aware that wireless networks with no required logins, can be easily sniffed by a stranger on

the same network.

13. **Do not open links or attachments in suspicious emails**
Be aware that even when they seem to be sent by someone you know, use caution as their email account might have been compromised by a hacker.
If in doubt, call the person or company to check first. Do not try emailing unless you can ask them for information only known to you both. Also do not trust any phone numbers in the email.

14. **Finally, use antivirus software, do not download pirated or cracked software as it can often contain malware**
Where available on iOS devices, use touchID and register multiple fingers.
Place tape over your webcam when not in use and use credit card online as you are then protected for purchases >100 and <30,000. Do not text or email your credit cards, bank account numbers, or passwords, no matter how much you trust the person on the other end. Keep your mobile device secure by using a strong password to lock it.

Kevin wrote on 'Will there always be cybercrime' in the August issue of MmIT Journal (Vol 42, No 3) and was a key note speaker on the topic at the 2016 MmIT Conference in September.

Kevin Curran *is*
Professor of Cyber Security and Group Leader for the Ambient Intelligence & Virtual Worlds Research Group, University of Ulster

MmIT Journal will be open access and in a new format from March 2017.
The journal interim editor is Leo Appleton. He can be contacted on: l.appleton@gold.ac.uk